T.C.
İSTANBUL ÜNİVERSİTESİ - CERRAHPAŞA
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

DOKTORA TEZİ

MİKRO DOPPLER RADARLAR TEMELLİ İNSAN TANIMLAMA SİSTEMLERİNDE ALDATMA SALDIRISI VE ÖNLEMLERİ

Muhammet Talha BÜYÜKAKKAŞLAR

DANIŞMAN
Doç. Dr. Muhammed Ali AYDIN

II. DANIŞMAN
Dr. Öğr. Üyesi Mehmet Ali ERTÜRK

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Doktora Programı

Eylül, 2024

TEZ KABUL VE ONAYI

Muhammet Talha BÜYÜKAKKAŞLAR tarafından, **Doç. Dr. Muhammed Ali AYDIN** danışmanlığında hazırlanan **"MİKRO DOPPLER RADARLAR TEMELLİ İNSAN TANIMLAMA SİSTEMLERİNDE ALDATMA SALDIRISI VE ÖNLEMLERİ"** başlıklı bu çalışma, jürimiz tarafından **16.09.2024** tarihinde yapılan sınav sonucunda oy birliği ile başarılı bulunarak **Doktora Tezi** olarak kabul edilmiştir.

Tez Jürisi

		İmza	Sonuç
DANIŞMAN	Doç. Dr. Muhammed Ali AYDIN İstanbul Üniversitesi-Cerrahpaşa Mühendislik Fakültesi		☐ Kabul ☐ Ret
ÜYE	Prof. Dr. Ahmet SERTBAŞ İstanbul Üniversitesi - Cerrahpaşa Mühendislik Fakültesi		☐ Kabul ☐ Ret
ÜYE	Prof. Dr. Selim AKYOKUŞ Medipol Üniversitesi Mühendislik ve Doğabilimleri Fakültesi		☐ Kabul ☐ Ret
ÜYE	Prof. Dr. Serhan YARKAN İstanbul Ticaret Üniversitesi Mühendislik Fakültesi		☐ Kabul ☐ Ret
ÜYE	Dr. Öğr. Üyesi Özgür Can TURNA İstanbul Üniversitesi - Cerrahpaşa Mühendislik Fakültesi		☐ Kabul ☐ Ret

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve bilimsel etik kuralları içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını ve her türlü hukuki sorumluluğu aldığımı kabul ederim.

Muhammet Talha BÜYÜKAKKAŞLAR

(İmza)

Aileme ithaf ediyorum...

BÜTÇE DESTEKLERİ

MİKRO DOPPLER RADARLAR TEMELLİ İNSAN TANIMLAMA SİSTEMLERİNDE ALDATMA SALDIRISI VE ÖNLEMLERİ

Bu tez çalışması için herhangi bir kurumdan bütçe desteği alınmamıştır.

TEŞEKKÜR

Doktora tez çalışmam süresince bilgi ve tecrübeleriyle bana yol gösteren ve yardımlarını esirgemeyen değerli tez danışmanlarım Doç.Dr. Muhammed Ali AYDIN'a ve Dr.Öğr.Üyesi Mehmet Ali ERTÜRK'e teşekkür ederim. Tez izleme komitemde yer alarak çalışmama fikirleri ile katkıda bulunan Prof.Dr. Selim AKYOKUŞ'a ve Dr.Öğr.Üyesi Özgür Can TURNA'ya saygı ve şükranlarımı sunarım. Siber Güvenlik/Kriptoloji alanında YÖK 100/2000 Doktora Bursu ile çalışmalarımı destekleyen Yükseköğretim Kurulu'na teşekkür ederim. Özellikle veri toplama aşamasında büyük destek veren Doç. Dr Vedat BEŞKARDEŞ'e gönülden teşekkürler ederim. İyi bir eğitim almam için maddi ve manevi desteklerini esirgemeyen sevgili aileme teşekkürlerimi bir borç bilirim.

Eylül 2024 **Muhammet Talha BÜYÜKAKKAŞLAR**

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

TABLO LİSTESİ

Sayfa No

SİMGE VE KISALTMA LİSTESİ

Simgeler **Açıklama**

$\mathbf{f_d}$: Doppler kayması
$\mathbf{\dot{R}}$: Hedef mesafesinin değişim oranı (hedefin hızı)
$\mathbf{f_0}$: İletilen sinyalin frekansı
$\mathbf{c}$: Işık hızı
$\mathbf{W}$: Kanalın geçiş olasılığı matrisi
$\mathbf{X}$: Giriş alfabesi
$\mathbf{S}$: Karıştırıcı durumlarının alfabesi
$\mathbf{Y}$: Çıkış alfabesi
$\mathbf{P}(\mathbf{Y})$: Çıkış olasılık dağılımı
$\mathbf{q}(\mathbf{s})$: Karıştırıcı durumunun olasılık dağılımı
$\mathbf{W_q}(\mathbf{y}|\mathbf{x})$: Ortalama kanal
$\mathbf{C}(\mathbf{W})$: Kanal kapasitesi
$\mathbf{F}(\mathbf{W})$: Kanalın simetrizasyon fonksiyonu
$\mathbf{U}$: Stokastik matris
$\mathbf{CH}(\mathbf{X};\mathbf{S})$: Giriş ve karıştırıcı durumları arasındaki kanal geçiş olasılığı fonksiyonları kümesi

Kısaltmalar **Açıklama**

FMCW : Frekans Modülasyonlu Sürekli Dalga
CW : Sürekli Dalga
ECM : Elektronik Karşı Önlem
ADAS : Gelişmiş Sürücü Destek Sistemleri
AI : Yapay Zeka
NB : Naive Bayes
SVM : Destek Vektör Makineleri
RTI : Radyo Tomografik Görüntüleme
DNN : Derin Sinir Ağı
TDNN : Zaman Gecikmeli Sinir Ağı

SVM-NB : Destek Vektör Makineleri - Naive Bayes
CNN : Evrişimsel Sinir Ağı
KNN : En Yakın Komşular Algoritması
PD : Darbe Doppler
BRB : Bayesyen Düzenlemeli Geri Yayılım
PRF : Darbe Tekrarlama Frekansı
SCG : Ölçekli Eşdönüşümlü Gradyan
LM : Levenberg-Marquardt
ANN : Yapay Sinir Ağı
YOLO : Bir kere bakarsın tipi yapay sinir ağı
DoS : Hizmet Reddi
PCA : Temel Bileşen Analizi
GMM : Gauss Karışım Modelleri
SVD : Tekil Değer Ayrışımı
HMM : Gizli Markov Modeli
Bi-LSTM : Çift Yönlü Uzun Kısa Süreli Bellek
MIMO : Çoklu Giriş Çoklu Çıkış
MISO : Çoklu Giriş Tekli Çıkış
SIMO : Tekli Giriş Çoklu Çıkış
SISO : Tekli Giriş Tekli Çıkış
ALEXNet : ALEXNet
ADA : Denetimsiz Düşman Etki Alanı Adaptasyonu
ASL : Amerikan İşaret Dili
HAR : İnsan Aktivitesi Tanıma
LASSO : En Küçük Mutlak Büzülme ve Seçim Operatörü
STFT : Kısa Zamanlı Fourier Dönüşümü
FFT : Hızlı Fourier Dönüşümü
DCNN : Derin Evrişimsel Sinir Ağları
LR : Doğrusal Regresyon
PR : Polinom Regresyonu
SVR : Destek Vektör Regresyonu

ÖZET

DOKTORA TEZİ

MİKRO DOPPLER RADARLAR TEMELLİ İNSAN TANIMLAMA SİSTEMLERİNDE ALDATMA SALDIRISI VE ÖNLEMLERİ

Muhammet Talha BÜYÜKAKKAŞLAR

İstanbul Üniversitesi - Cerrahpaşa

Lisansüstü Eğitim Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Muhammed Ali AYDIN

II. Danışman: Dr. Öğr. Üyesi Mehmet Ali ERTÜRK

Bu tez, mikro doppler radar tabanlı insan-hayvan ayrımı yapan sistemlerde aldatma(spoofing) saldırılarına odaklanmaktadır. Temel teori, radar sistemlerinin bir iletişim kanalı olarak modellenebileceği yönündedir. Bu nedenle literatürde daha önceden gösterilmiş olan bir iletişim kanalında aldatma (spoofing) veya karıştırma (jamming) saldırısını algoritmik olarak tespit etmenin imkansız olmasının radar sistemleri için de geçerli olması gerekmektedir. Bu durumun temel sebebi bir iletişim kanalında karıştırma saldırısının tespiti probleminin durdurma (halting) problemi ile eşlenik olmasıdır. Bu nedenle, tez, sezgisel yöntemlerin bu tür saldırıların tespiti ve direnç sağlanması olgusunu araştırmaktadır. Bu teorik çerçeve matematiksel olarak ifade edilmiştir. Ardından teorik çerçeveyi doğrulamak için deneysel yöntemlerle gösterim yapılmıştır. Bu gösterimi yapmak için daha önceden yayınlanmamış nitelikte bir veri seti tasarlanmıştır, ardından bu veri setinin gerçekleştirilmesi ve mikro doppler radar tabanlı bir insan-hayvan sınıflandırma sistemi geliştirilmesi sağlanmıştır ve bu sistem üzerinde karıştırma saldırıları gerçekleştirilmiştir. Saldırı tespit ve teşhis mekanizmaları tasarlanmış ve insan/hayvan ayrım algoritmaları, saldırı altında bile çalışabilme yeteneğini artırmak için güncellenmiştir. Bu tez kapsamında elde edilen çıktılar şu şekildedir; teorik altyapının oluşturulması için öncelikle fiziksel katman itibariyle radar iletişim sistemlerinin bir iletişim katmanı olarak modellenebileceği gösterilmiştir. Ardından yenilikçi bir veri seti toplanarak literatürde ilk defa bir çok hayvan cinsinin bir arada olduğu bir veri seti toplanarak gelecek araştırmalar için de bir altyapı sağlanmıştır. Ardından klasik bir radar izi tanımlayıcı gerçeklenmiş ve buna klasik karıştırma saldırılarından biri ile saldırı yapılmıştır. Son aşamada bu saldırıların tespit edilmesi ve saldırılara direnç gösterilmesi için yenilikçi bir yapay zeka sistemi tasarlanmıştır.

09/2024, 97 sayfa.

Anahtar kelimeler: Frekans Modülasyonlu Sürekli Dalga Radarları, İnsan Tanıma, Mikro-Doppler Radarlar, Aldatma Saldırıları.

ABSTRACT

Ph.D. THESIS

SPOOFING ATTACK ON DOPPLER RADAR BASED HUMAN CLASSIFICATION SYSTEMS

Muhammet Talha BÜYÜKAKKAŞLAR

İstanbul University - Cerrahpaşa

Institute of Graduate Studies in Sciences

Department of Computer Engineering

Supervisor: Assoc. Prof. Muhammed Ali AYDIN

Co-Supervisor: Asst. Prof. Mehmet Ali ERTÜRK

This thesis focuses on spoofing attacks in micro-Doppler radar-based human-animal classification systems. The fundamental theory is that radar systems can be modeled as a communication channel. Therefore, the impossibility of algorithmically detecting spoofing or jamming attacks in a communication channel, as shown in the literature, should also apply to radar systems. The main reason for this is that the problem of detecting jamming attacks in a communication channel is analogous to the halting problem. Hence, this thesis investigates intuitive methods for detecting and resisting such attacks. This theoretical framework is expressed mathematically, followed by experimental demonstrations to validate it. To conduct these demonstrations, an unpublished dataset was designed, implemented, and used to develop a micro-Doppler radar-based human-animal classification system, where jamming attacks were conducted on the system. Detection and diagnosis mechanisms for the attacks were designed, and human/animal classification algorithms were updated to enhance their ability to function under attack conditions.The findings obtained in this thesis are as follows: First, it was demonstrated that radar communication systems can be modeled as a communication layer from the physical layer perspective to establish the theoretical basis. Next, an innovative dataset was collected, which, for the first time in the literature, includes various animal species, providing a foundation for future research. Then, a classical radar signature classifier was implemented, and it was subjected to a classical jamming attack. In the final stage, an innovative artificial intelligence system was designed to detect these attacks and resist them.

09/2024, 97 pages.

Keywords: Frequency-Modulated Continuous Wave Radars, Human Recognition, Micro-Doppler Radars, Spoofing Attacks.

1. GİRİŞ

Radar kelimesi ingilizcede "Radio Detection and Ranging" - Radyo Algılama ve Mesafe Belirleme, tabirinin kısaltması ile oluşturulmuştur. Radarlar radyo dalga kullanarak nesnelerin konum, hız, ve yönünü tespit etmekte kullanılır. Radar sistemler bir radyo dalgası yayınlayıp geri dönüş ekosunu dinleyerek çalışır. Geri dönüş sinyalinin yapısına göre radar sistemler hedeflerin tanımlaması ve takibini yapabilir.

Radar sistemlerin kullanım alanları oldukca geniştir. Bu alanlar arasında hava trafik kontrolü, hava durumu takibi, askeri alanlar, ve denicilik uygulamaları sayılabilir. Bu çalışmanın içeriğinde insan tespit ve sınıflandırma sistemleri uygulamaları üzerine yoğunlaşılacaktır. Bu tip radarlar genelde araçlarda FMCW radar olarak, sağlık sektöründe hasta gözetleme için, ve güvenlik sistemlerinde kullanılmaktadır.

Radar sistemlerin sinyal işlemesi ve veri analizinde yapay zeka teknolojilerinin ciddi avantajları mevcuttur. Otomatik hedef tanıma, gelişmiş adaptasyon yetenekleri, öğrenme yetenekleri, siber güvenlik düzeyi, kaynak optimizasyonu, ve yeni teknolojilere entegrasyon kolaylığı bu avantajlar arasında sayılabilir. Yapay zeka destekli radarlar gelişmiş hedef tespiti, ve tanımlama doğruluğu, enerji optimizasyonu ve doğru band genişliği kullanımı ile siber saldırılara karşı yüksek dayanım gösterirler.

Karıştırma (Jamming) ve aldatma (spoofing) saldırıları radar sistemlerinin güvenilirliğini ve doğruluğunu ciddi olarak etkileyebilirler. Karıştırma saldırıları diğer radyo sinyallerini bozmak ve bloklamak için güçlü saldırgan sinyaller yayınlamak yoluyla yapılır. Bu tip saldırılar radarların hedefleri tespit ve takip edebilmelerini oldukça zorlaştırırlar bu yolla radar sistemlerinin güvenilirliğini ve etkinliğini düşürürler. Karıştırma saldırıları askeri ve sivil sistemler için ciddi tehtit oluştururlar. Askeri sistemlerde karıştırma saldırıları düşman tespitini engelleyebilir. Sağlık sektöründe ise genelde bu tip saldırılar

özellikle amaçlanmasa bile, çevrede bulunan nesneler tarafından istenmeden oluşan karıştırma etkileri gözlenebilir.

Aldatma saldırıları radar sistemlerine sahte sinyaller göndererek gerçek hedeflerin konumunu ve karakteristik özelliklerini gizlemeyi amaçlar. Bu tip saldırılar genelde saldırgan tarafından hedef radarı yanlışa yönlendirecek sinyaller yayınlanmasıyla yapılır. Aldatma saldırıları bu yayınlanan sinyaller sayesinde saldırdıkları radarların hedeflerini tespit etmesini engellemeyi, hedefin tipinin yanlış sınıflandırılmasını, veya hiç var olmayan bir hedefin sistemde gösterilmesini sağlamayı amaçlar. Askeri uygulamalarda düşmanın yerini veya kimliğini yanlış algılayan radar bu düşmanı dost olarak görebilir, tehtid olmayacak kadar uzakta zannedebilir veya var olmadığı bölgede düşman var zannederek karşı önlem imkanlarını tüketebilir. Sivil uygulamalarda ise aldatma saldırıları sayesinde otomobillerin FMCW radarları aldatılarak hedef otomobillerin ani fren yapması veya frenleme yapması gereken yerde yapmaması sağlanarak kazalara sebep olunabilir. Bu gibi durumların tamamı hedefler için ölümcül olma potansiyeline sahiptir.

Karıştırma ve aldatma saldırılarına karşı koyak ve radar sistemlerini bu salsdırılara daha dirençli hale getirmek için şu önlemler alınmaktadır;

Frekans zıplamalı radar teknolojisi: Zıplamalı Frekans radar teknolojileri kullanılarak karıştırma ve aldatma saldırılarının etkileri azaltılabilir. Frekans zıplama tekniklerinin kullanımı sayesinde saldırgan radarların kullanılacak frekans aralığını tahmin etmesi, bozucu veya aldatıcı yanıt frekansı yayınlaması zorlaştırılır.

Yapay Zeka ve Makine Öğrenmesi Teknikleri: Yapay zeka ve makine öğrenmesi teknikleri sayesinde gelen radar sinyalleri analiz edilerek bozucu sinyallerin izole edilmesi ve etkisinin azaltılması mümkündür.

Sinyal işleme ve veri analizi: Gelişmiş sinyal işleme ve veri analizi teknikleri radarların karıştırma ve aldatma saldırılarına karşı daha dirençli olmasını sağlayacaktır. Sinyal işleme teknikleriyle saldırganların ürettiği sinyallerin tanımlanması etkilerinin yok edilmesi ve üst katman analizlerin daha güvenilir

bir şekilde yapılmasının sağlanması mümkündür.

Çoklu-sensor Entegrasyonu: Birçok sensörün entegre edilmesi ve destekleyici bir katman olarak bu sensörlerle yapılacak bir sensör füzyon saldırganların tespitini kolaylaştıracaktır. Saldırganların bir tip sensöre saldırması ve diğer tip sensörlere aynı etkinlikte saldıramaması durumunda bu sensörler arasında tutarsızlık oluşması saldırgan tespitini sağlayacaktır. Ayrıca bu şekilde bir sensör füzyon desteği sağlanması radar sistemlerinin hedef tespit ve tanımlama menzillerini arttıracaktır.

İşbirliği Yapan Radar Sistemleri: Bir çok radar sistemi arasında veri paylaşımı yapmak karıştırma ve aldatma saldırılarına karşı dah iyi savunma sağlar. İşbirlikci radar sistemleri birlikte çalışarak hedefleri takip edebilir, yüksek hedef tespit oranına ulaşır, ve daha iyi karıştıma dayanıklılığına sahip olur. İşbirliği yapan radar sistemlerinde kullanılan alt sistemlerin yarısı dahi saldırıdan etkilense bile diğer yarısından gelen verilerle doğru hedef tespitinin yapılması mümkündür.

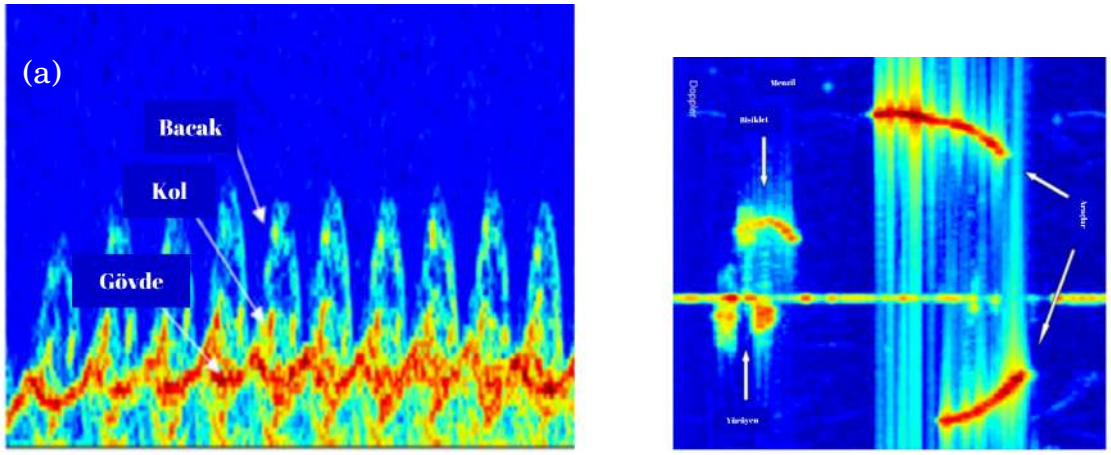
Tahmoush ve Silvious un 2009 da yaptığı çalışma doppler radar sinyallerinde insan ve hayvan ayrımının yapılması üzerinedir[1]. Bu çalışmada deney düzeneği yerine simule edilmiş sinyal çıktıları çalıştırılmıştır. Bu çalışma sonucunda elde edilen sonuçlarda bu işlemin fizibil olarak yapılabileceği, sinyallerden gövde, sallanan kollar, ayaklar gibi özelliklerin çıkartılabileceği gösterilmiştir.

Bu çalışmalar genellikle bu alanda daha önce gerçekleştirilmiştir. Bu bölümde listelenen çalışmalar, genellikle mikro-doppler radarlarının insan aktivitelerini tanıma konusundaki uygulanabilirliğiyle ilgilenmektedir. Lai [2] bu alandaki erken çalışmalardan birini yapmıştır. Lai, binaların içindeki insanları gözetlemek için rastgele gürültü mikro doppler radarının kullanılabilirliğini araştırmıştır. Bu çalışma, mikro-doppler radarının güvenlik amaçlı bir kullanımı olarak da sınıflandırılabilir, çünkü aracın gözetim uygulamasıyla ilgilenmektedir. Li, doktora tezinde [3] rastgele gürültü radarı kullanarak bir duvarın içini gözlemleme olasılığını araştırmıştır. Deneysel çalışmada, bu süreç yüksek bir performansla gerçekleştirilmiştir.

Tahmoush ve Silvous[1] bu alanda erken bir çalışma yapmışlardır. 2009 yılında Tahmoush ve Silvious, doppler radar sinyalleri kullanarak insan ve hayvan ayrımına odaklanmıştır. Bu çalışmada, deneysel kurulum yerine simüle edilmiş sinyal çıktıları kullanılmıştır. Bu çalışmanın sonuçları, bu işlemin uygulanabilir olduğunu ve gövde, sallanan kollar ve ayaklar gibi özelliklerin sinyallerden çıkarılabileceğini göstermektedir. Araştırmalarının bir devamı olarak, Tahmoush ve Silvious, mikro-doppler radarlarında açı, amplitüd, PRF ve aydınlatmanın önemini araştırmışlardır [4]. Bu araştırma ile hareket açısının radar açısından en önemli faktörlerden biri olduğunu göstermişlerdir.

Bryan ve diğ. [5] doppler radar izi kullanarak insan davranışını tanımlama konusunu ele almışlardır . Bu çalışmada geliştirilen SVM kullanılarak yürüme, koşma, dönme, yumruk atma, zıplama, oturma, ayakta durma, emekleme ve ayakta kalma hareketleri tanımlanmıştır. Bu öncü çalışmanın alanda daha fazla geliştirilmesi gerekliliği, Sonuçlar bölümünde vurgulanmıştır. Özellikle, radarın tersi yönde yapılan hareketlerin ve yatay alandaki performans düşüşünün, yazarların en çok üzerinde durduğu eksiklikler olduğu belirtilmiştir.

Gürbüz ve diğ. [6] simüle edilmiş radar sinyallerini araştırmışlardır. Bu çalışmada, radara 90 derece açıyla karşıdan koşan ve yürüyen 16 kişinin hareketleri değerlendirilmiştir. Veri setinin küçük boyutu nedeniyle, bu çalışmanın daha büyük veri setleriyle gerçekleştirilmesi, sonuçların daha net bir şekilde değerlendirilmesini sağlayacaktır.



Şekil 1.1: a) Yürüyen insan doppler radar izi, b) Bisikletli ve araç doppler radar izi

Narayanan ve diğ. [7], 18 farklı insan aktivitesinin 6.5 Ghz mikro-doppler radar izini incelemişlerdir. Bu hareketleri doğru bir şekilde sınıflandırmak için çeşitli özellikler ve çıkarım yöntemleri üzerinde çalışmışlardır.

Chenye Li'nin yüksek lisans tezi, ultrasonik sensörler kullanarak yapılan bir yürüme analizi çalışmasını içermektedir [8]. Li, ses sinyallerinin ultrasonik yürüme doppler etkisine dayanan sensörleri kullanmıştır. Bu çalışmada kullanılan ortam radar sinyalleri yerine ses sinyallerinden oluşsa da, doppler etkisi nedeniyle ana aktif faktörler dikkate alınmıştır. Bu çalışmanın sonucunda, Maksimum Ayak Hızı, Yerde Kalma Süresi, Ayak Sallanma Süresi, Yürüme Döngü Süresi, Sallanma/Durma Oranı, Durma Oranı, Dakikadaki Adım Sayısı, Adım Uzunluğu, Ortalama Adım Oranı, Her İki Ayakta Yerde Kalma Süresi, Simetri İndeksi, Yürüme Hızı gibi değerler elde edilmiştir.

2. KAVRAMSAL ÇERÇEVE

2.1. RADAR TİPLERİ

İnsan tanıma sistemlerinde farklı türde radarlar kullanılabilir. Bu nedenle, çeşitli radar türlerine dayanan makaleler incelenmiştir. Farklı radar türleri, kendine özgü yeteneklere ve dezavantajlara sahiptir. Ayrıca, radar türüne bağlı olarak veri türü oluşturma desenleri farklılık göstermektedir. Bu nedenle, veri işleme ve radarlar üzerindeki aldatma ve karıştırma gibi saldırıların doğası da değişmektedir.

2.2. MODÜLE OLMAYAN SÜREKLİ DALGA RADARLARI ÇALIŞMA PRENSİPLERİ

Modüle edilmemiş CW radarlar, hedefleri tespit etmek için belirli bir frekansta sürekli olarak yayın yapar [9]. CW radarın temel çalışma prensibi, belirli bir frekanstan radyo dalgalarının sürekli olarak iletilmesine dayanır. Bu dalgalar, gözlemlenmek istenen alana yönlendirilir. İlgili alana giren dalgalardan hedefe çarpan kısım yansıtılır. Alıcı anten, geri dönen dalgaları algılar ve bu şekilde hedefe ilişkin bilgi elde eder.

CW radarların başlıca avantajı, basit yapıları sayesinde kolayca üretilebilmeleridir. Dezavantajları arasında ise sabit nesneleri tespit edememe ve tespit ettikleri nesneler arasındaki mesafeyi belirleyememe yer alır.

Bu denklem, doppler kaymasını, hedefin hızı, iletilen sinyalin frekansı ve ışık hızı ile ilişkilendirir.

$$f_d = \pm \frac{2\dot{R} f_0}{c} \tag{2.1}$$

[9]

Eğer hız $\dot{R}$ bu denklemden çıkarılırsa, hız şu şekilde belirlenir:

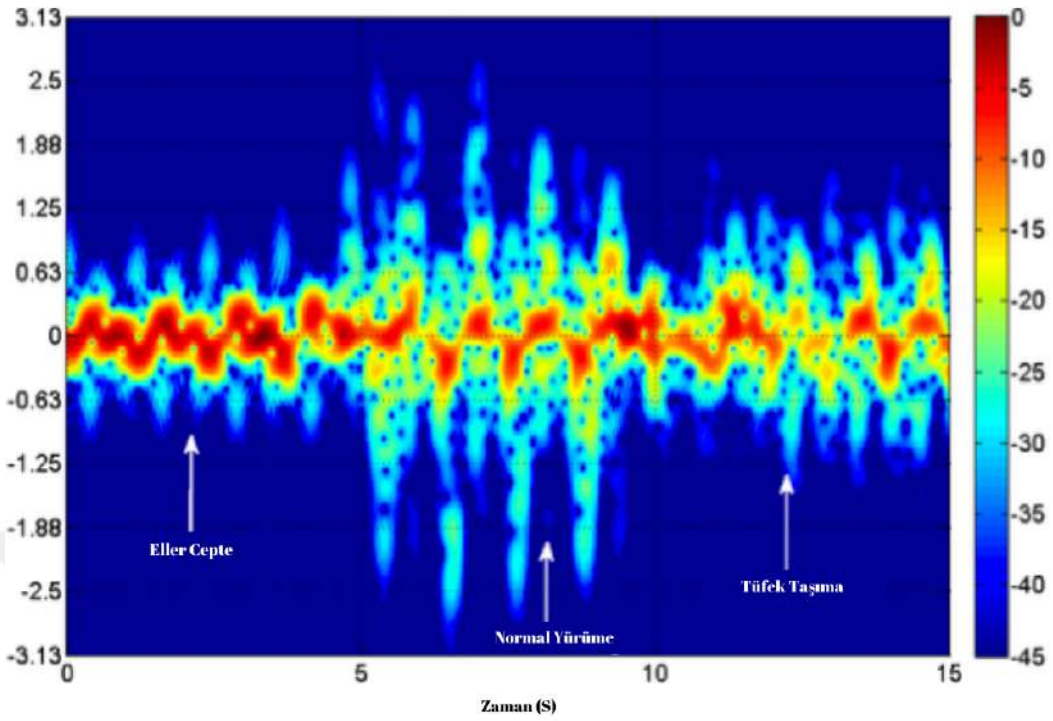
$$\dot{R} = \pm\frac{cf_d}{2f_0} \tag{2.2}$$

CW radarlar, insan ve hayvan aktivitesi tanıma sensörleri olarak uygulanmıştır. CW, insan aktivitesi tanıma teknikleri alanında FMCW ile birlikte en çok kullanılan iki radar türünden biridir. Literatürde, CW radarlar tipik olarak sabit kurulumlar için kullanılır. Bu kurulum türü tercih edilir çünkü CW radarların hareketli kurulumlarında arka planı hedeften ayırmak çok zordur. Fioranelli ve diğ., MISO-CW radar kullanarak çeşitli çalışmalar yapmışlardır. Bu çalışmalardan dördü, yürüyen bir kişinin tüfek taşıyıp taşımadığını belirlemiştir [10–13]. **Şekil 2.1** ve **Şekil 2.2** de gösterildiği gibi, bu çalışmalar yürüyen kişinin tüfek taşıyıp taşımadığını, yürürken sallanan ellerine bağlı olarak ayırt etmektedir. Bu özelliğe bağlı olarak, algoritmaların gerçek hayattaki uygulamaları engellenebilir. Çünkü metal nesneler, insan vücuduna kıyasla RF sinyalinin daha güçlü yansıma gücüne sahiptir ve bu özellik, silahlı hedeflerin sınıflandırılmasında kullanılabilir. Ayrıca topallayan hayvanları tespit etmek için de çalışmalar yapılmıştır. Fioranelli ve Shrestha'nın da dahil olduğu benzer ekipler [14–16] benzer donanımlar kullanarak, CW radarlar gibi, bu çalışmaları gerçekleştirmiştir. Bu çalışmalar, at, inek ve koyun gibi hayvanların topallığını tespit ederek hayvan bakım uygulamalarında CW radarları içermektedir.

2.3. ATIM DALGA RADARLARI ÇALIŞMA PRENSİPLERİ

PD radarlar, radyo dalgalarını aralıklı olarak ileterek çalışır. Bu yayın gruplarının her biri bir "beat" olarak adlandırılır. PD radarlar, kontrol edilen alandaki hareketli ve sabit hedeflerin hızını ve mesafesini ölçebilir. Hedefler arasındaki mesafeyi belirlemek için darbelerin geri dönüş süreleri ölçülür. Hedefin hızı, iletilen dalganın frekans kaymasından belirlenir.

Darbe doppler radarının en önemli avantajlarından biri, sabit hedefleri tespit edebilme yeteneğidir. Bu yöntemlerin bir diğer önemli özelliği ise yüksek çözünürlükleridir. Sonuç olarak, PD radarlar hedeflerin hızını ve mesafesini



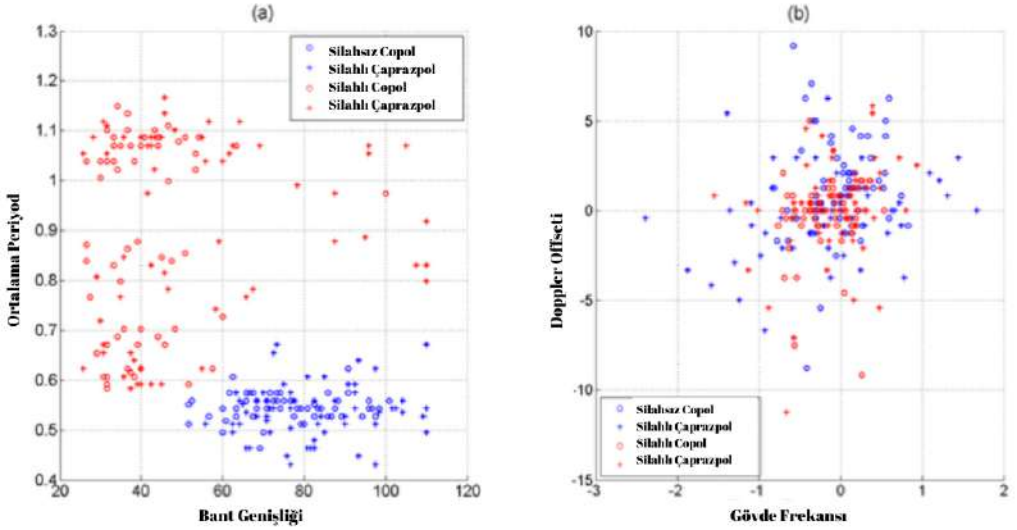
Şekil 2.1: Eller ceplerde yürüyen, normal yürüyen ve tüfek taşıyan kişilerin spektrogram analizi.

yüksek bir hassasiyetle ölçebilir.

$$\triangle\Theta = \frac{4\pi v \triangle t}{\lambda} \tag{2.3}$$

$$v = \frac{\lambda \triangle\Theta}{4\pi \triangle t} \tag{2.4}$$

[17] PD radarlarının insan aktivitesi tanıma amacıyla kullanılabilirliği üzerine yapılan çalışmalar sınırlıdır. Gürbüz ve diğ. kapalı alan aktivitelerini tanımada 3 farklı radar türünü ve sonarı karşılaştırmıştır. Bu çalışma, SNR oranları, fiyatlandırma, sinyal kalitesi ve sınıflandırma verimliliğini değerlendirmiştir. Çalışmaları, birkaç açıdan daha iyi alternatiflerin mevcut olduğunu göstermektedir. Bu faktörler, bu alandaki çalışmaları sınırlamış



Şekil 2.2: Tüfekle ve tüfeksiz yürüyen bir kişinin dağılım analizi.

olabilir.

PD radarlarını verimli bir şekilde sınırlamak için karıştırma etkileri ve stratejileri üzerine iki çalışma yapılmıştır [18, 19]. Bu çalışmalar, PD radarlarına karşı başarılı aldatma saldırılarını gösterme açısından önemlidir.

2.4. MODULE SÜREKLİ DALGA RADARI ÇALIŞMA PRENSİPLERİ

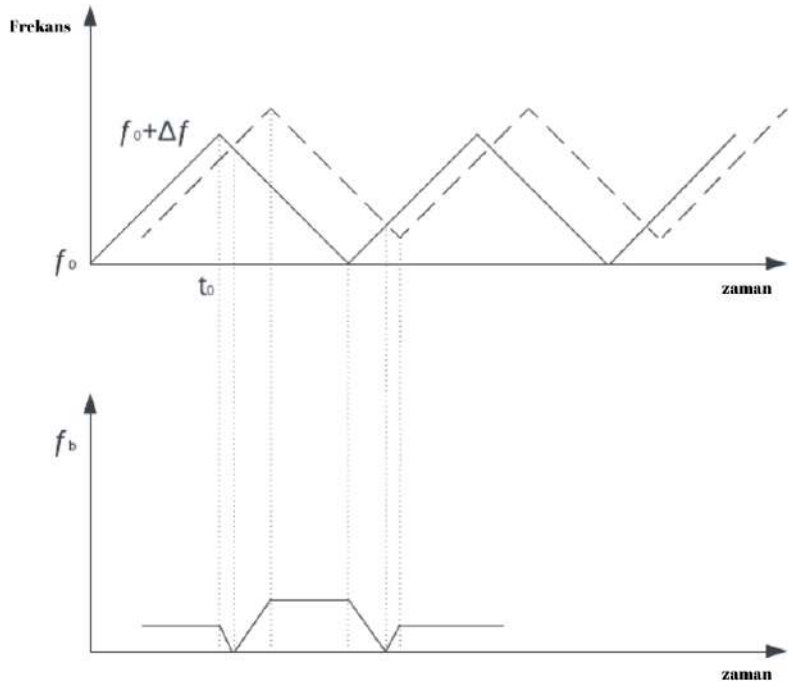
FMCW radarlar, sürekli yayın yapan radar türlerindendir. FMCW radarlarının temel çalışma prensibi, frekanslarını düzenli bir desende değiştirerek yayın yapmaktır. Bu yayının geri bildirimini dinlemek, hedefin mesafesi ve hızı hakkında bilgi taşır.

FMCW radarlarının avantajlarından biri, sabit nesneleri tespit etme yeteneğidir. Hedefin hızı, geri dönen sinyalin doppler etkisi hesaplanarak belirlenebilir. Yayının, nesneden dönen frekansı ve hedefin mesafesi tespit edilebildiğinden, geri dönen sinyalin doppler etkisi hesaplanarak hedefin hızı

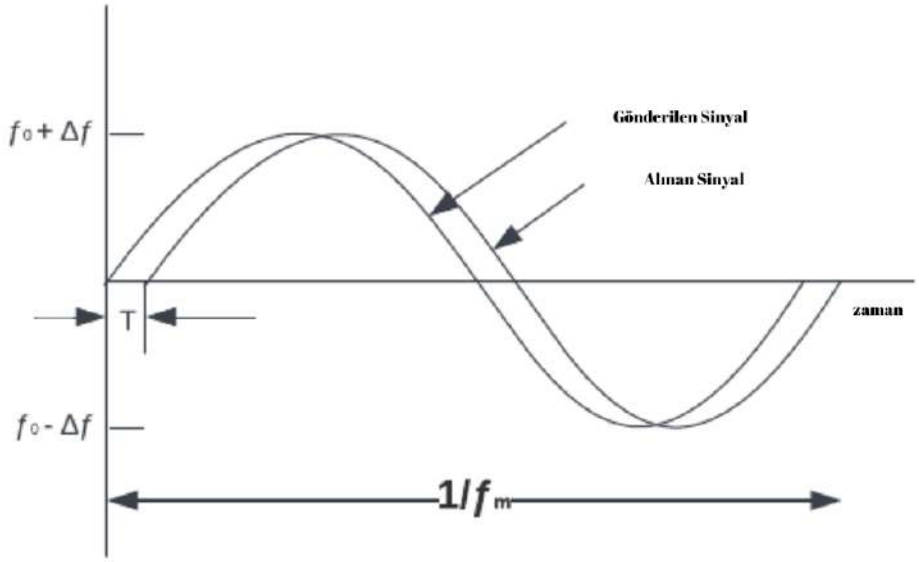
belirlenebilir.

FMCW radarlarının bir diğer avantajı, modüle edilmiş frekanslarda çalışmaları sayesinde hız veya mesafedeki küçük değişiklikleri yüksek çözünürlükle tespit edebilmeleridir. FMCW radarlar, aynı anda birçok hedefin takibini sağlar. Bir yayın deseni, nesneler arasındaki hız ve mesafeyi gizleyebilir. Bu nedenle, FMCW radarına dayalı sistemler, birçok nesneyi aynı anda tespit edip izleyebilir.

FMCW radarlarının iki temel türü vardır: lineer ve sinüzoidal FMCW radarlar. Lineer FMCW radarlar, **Şekil 2.3**'de gösterildiği gibi doğrusal olarak değişen çıkış sinyalleri üretir. Hedefe ait bilgi, üretilen sinyalin geri dönüşünde meydana gelen doppler kayması yoluyla elde edilir. Sinüzoidal FMCW radarlarında, **Şekil 2.4**'de gösterildiği gibi sinüzoidal bir sinyal üretilir. FMCW radar kullanarak, hedefin mesafesi ve hızı hakkında bilgi elde edilebilir.



Şekil 2.3: Lineer FMCW Prensipleri



Şekil 2.4: Sinüzoidal FMCW Prensipleri

Hedefin uzaklığı şu şekilde hesaplanır:

$$R = \frac{c}{4\dot{f}_c}(f_b{}^- - f_b{}^+) \tag{2.5}$$

Hedefin hızı şu şekilde hesaplanır:

$$\dot{R} = \frac{\lambda}{4}(f_b{}^- - f_b{}^+) \tag{2.6}$$

FMCW radarlarının sağlık sektörü ve yaşlı bakımı alanında kullanımıyla ilgili literatür, CW radarlarının kullanımına kıyasla sınırlıdır. Bu durum, CW radarlarının yeterli kabiliyetine veya FMCW radarlarının sabit nesneleri tespit edebilme yeteneğine bağlı olabilir. Ana hedefin düşme tespiti olduğu durumlarda, bu durum gereksiz bir bilgi akışına neden olabilir. Ancak, bu konuda çeşitli çalışmalar yapılmıştır. Bhattacharya ve diğ. [20], insan düşme tespiti için bir FMCW radar sistemi geliştirmiştir. Bu çalışmanın önemi, CNN yapısı olan RadarNet'te yatmaktadır. Bu yenilikçi radar sistemi, FMCW radar verilerini kullanarak insan aktivitesini tespit etmektedir. Diğer çalışmalar,

FMCW radarları kullanarak düşme tespiti üzerinde yoğunlaşmıştır [21, 22]. Bu çalışmalarda, düşmeleri daha doğru bir şekilde tespit etmek için sensörler, giyilebilir sensörlerle birleştirilmiştir.

Vandermissen ve ekibi bu alana özgün bir katkı yapmıştır. Bu çalışmalar, kapalı ortamlarda belirli insanları tanımlamayı amaçlamıştır [23]. Bu, sınırlı bir insan veri tabanı kullanılarak gerçekleştirilmiştir. Ancak, insan veri tabanı sınırlı olsa bile, bu çalışma, erişimi kısıtlı alanlarda insanları tanımlamak gibi gerçek dünya uygulamaları için umut vaat etmektedir, böylece seçenekler sınırlandırılabilir. Vandermissen'in bir diğer çalışması, el sallama, vurma, kaydırma gibi el hareketlerini tespit etmektir [24].

Araçlarda kullanılan FMCW radarlarının kullanımı her geçen gün artmaktadır. Bu olguya paralel olarak, bu radarların kullanımıyla ilgili araştırmalar, bu radarların sınırlı yeteneklerine yönelik saldırı türleri ve karşı önlemlerle ilgili çalışmalar kadar artmaktadır.

Tablo 2.1: Yapay zeka tekniklerine odaklanan yayınlar.

Yayın	Radar Tipi	Sınıflandırma	YZ Tekniği
[25]	CW	İnsan Yürüyüşü	CNN, LSTM
[26]	CW	İnsan Aktiviteleri	DNN
[14–16]	CW	Hayvan Topallığı	KNN, NB
[27]	CW	İnsan Solunum Sistemi	SVM
[28]	CW	Bisiklet, Araba, İnsan, Ağaç, Köpek	DNN, SVM, NB
[20]	CW	İnsan Düşme Tespiti	CNN
[29]	CW	El Hareketleri	SVM
[30]	CW	İnsan Aktiviteleri, Kimlik Tespiti	CNN
[31]	CW, PD	Topallama, baston, yürüme, tekerlekli sandalye	SVM, NB
[10]	CW, MISO	Tüfekli ve Tüfeksiz İnsan	PCA, SVD
[11–13]	CW, MISO	Tüfekli ve Tüfeksiz İnsan	NB
[32]	FMCW	Birden Fazla Yaya ve Nesne	DT, CDMC
[21]	FMCW	Farklı İnsan Aktiviteleri	Bi-LSTM DNN
[33]	FMCW	İnsan Tespiti	GA, RS, SVM
[34]	FMCW	İnsan, Araç, Bisikletli	SVM
[35–37]	FMCW	İnsan, Araç, Bisikletli	CNN
[38]	FMCW	İnsan Yörüngeleri, Nefes Alma	Bi-LSTM
[39]	FMCW	Araba, Yaya, Bisikletli, Köpek	CNN
[40]	FMCW	Düşme, Oturma, Ayakta Durma	KNN
[41]	FMCW	Araç, Yaya	SWVM-YOLO
[42]	FMCW	Araç Genişliği	RF
[24]	FMCW	El ve Yürüyüş Aktiviteleri	LSTM, CNN
[22, 43]	FMCW	Kapalı Alanda İnsan Aktiviteleri	Bi-LSTM

Tablo 2.2: Mikro-doppler radar sensör füzyon tekniklerine dair yayınlar.

Yayın	Radar Tipi	Sınıflandırma	Füzyon Tekniği
[25]	CW	CNN, RNN, LSTM	Kamera
[21]	FMCW	Bi-LSTM	Akıllı Bileklik
[44]	CW	R-CNN	Kamera
[45]	FMCW	NA	LiDar / Kamera
[46]	NA	$H\infty$	Radar-Radar
[24]	FMCW, CW	DNN, LSTM, CNN-LSTM, 2D CNN	Kamera
[31]	CW, PD	SWM, NB	CW Sonar
[41]	FMCW	SWVM-YOLO	YOLO-SVM

Chenye Li'nin [8] yüksek lisans tezinde ultrasonik sensorler kullanarak yaptığı yürüyüş analiz çalışması bulunmaktadır. Bu çalışmada Li ultrasonik kişinin yürüyüşünün ses sinyaller üzerinde oluşturduğu doppler etkisinin ölçülmesine dayanan sensörler kullanarak çalışmasını yapmıştır. Yapılan çalışmada kullanılan ortam radar sinyalleri yerine ses sinyalleri olmakla beraber temel etken faktörler dopler etkisi olması dolayısıyla çalışmamızda dikkate alınmıştır. Bu çalışma sonucunda Pik Ayak Hızı, Ayağın Yerde Kalma Süresi, Ayak Sallanma Süresi, Yürüşüş Döngü Süresi, Sallanma/Durma Oranı, Durma Oranı, Dakikadaki Adım Sayısı, Adım Uzunluğu, Ortalama Adım Hızı, İki Ayağında Yerde Kalma Süresi, Simetri İndexi, Yürüyüş Hızı, Yürüme Oranı değerlerini çıkartmıştır.

Narayanan ve Zenaldin'in [7] çalışmasında yapılan araştırma doopler radar ile insan hareketlerinin tanımlanması ve özellik çıkarımı üzerine olmuştur. Bu çalışmanın bir diğer kayda değer yönü duvar arkasından görüntülemenin etkisi de araştırılarak bu analizlere dahil edilmiş olmasıdır. Çalışma duvarın etkisini sinyal gücünü sönümleyici olmakla beraber yapısal olarak ciddi bir değişimin olmadığını göstermiştir.

Damarla ve diğ. [62] yaptıkları çalışmada insan ve at sinyallerinin ayrımı ile ilgilenmişlerdir. Veri seti toplamak amacıyla bir hara da insanların ve atların doppler Radar önünden geçmeleri sağlanmıştır. Bu veriler işlenerek yüksek ve düşük SNR değerlerinde (hedefin uzak veya yakın olduğu durumlarda) kullanılmak üzere iki farklı sınıflama algoritması gerçeklemişlerdir.

Tablo 2.3: Aldatma saldırılarına odaklanan yayınlar.

Yayın	Radar Tipi	Sınıflandırma	Aldatma Tekniği
[47]	CW	NA	Geri Saçılma Saldırısı
[45]	FMCW	Araç, Hız	Geri Saçılma Saldırısı
[46]	NA	Araç, Hız	Sensör Seviyesi Saldırısı
[48]	FMCW	NA	Tekrar Oynatma Saldırısı
[49]	FMCW	Araç, Hız	Düşman Sinyali
[50]	FMCW	Araç, Hız	Sensör Saldırısı, Sistem Seviyesi Saldırısı, Düşman Sinyali
[18]	PD	Hedef	Karıştırma Sinyali
[51]	FMCW	Yürüyen İnsan, Duvar Arkası, Duran İnsan	Düşman Sinyali
[52]	FMCW	Duran İnsan	Düşman Sinyali
[53]	FMCW	Genel Nesne	Geri Saçılma Saldırısı
[54]	FMCW	Genel Nesne, Mesafe	Tekrar Oynatma Saldırısı
[55]	FMCW		Düşman Sinyali
[56]	-	Aldatma	Sistem Seviyesi Saldırısı
[38]	FMCW	İnsan Yörüngeleri, Nefes Alma	Dinleme
[57]	MMW Radar	Nesne	Sistem Seviyesi Saldırısı
[58]	MMW Radar	Nesne	Sistem Seviyesi Saldırısı
[59]	FMCW	Nesne/Araç	Sensör Saldırıları
[60]	CW	Tüfek ve Çantalarla Yürüyen İnsan	Karıştırma Saldırıları
[61]	CW	Tüfek ve Çantalarla Yürüyen İnsan	Karıştırma Saldırıları

Villeval ve diğ. [63] otomotiv standardı doppler radar kullanarak insan tespiti yapmak üzerine çalışmışlardır . Bu çalışmanın özelliği gerçek şehir ortamı simule ediğidiği için etraf gürültüsünün yüksek olduğu, insan davranışlarının çok net olmadığı bir ortamda yapılmış olmasıdır. Çalışmada insan köpek ve araçlar başarılı olarak sınıflandırılmıştır.

Gürbüz ve diğ. [6] simule edilmiş radar sinyalleri üzerine çalışmıştırlar. Bu çalışmada koşan ve yürürüyen 16 kişinin radarlara karşı ve radarlara 90 derece açı ile yaptıkları hareketler değerlendirilmiştir. Veri setinin küçük olması nedeniyle bu çalışmanın daha geniş veri setleri ile yeniden yapılması sonuçların daha net şekilde değerlendirilmesini sağlayacaktır.

Arık ve diğ. [64] yaptığı çalışmada çeşitli sınıflama algoritmalarının doppler radar sinyalleri sınıflandırılmasında kullanılarak karşılaştırılması yapılmıştır. Bu çalışmada kullanılan algortimalar şunlarıdır; Scaled Conjugate Gradient (SCG), Levenberg-Marquardt (LM) ve Bayesian Regularization Backpropagation (BRB). Sonuç kısımında yazarlar bu algoritmaların işlem zamanlarının yüksekliği ve gerçek zamanlı uygulamalarda kullanılması için yeniden elealınması gerekliliğini vurgulamışlardır.

Jong ve diğ. [25] çalışmasında doppler Radar izi ve Kamera görüntüsü için sensor füzyon algortimaları geliştirilmiştir. Özellikle insan tanımlama algoritmaları için geliştirilen bu füzyon teknikleri data seviyesi, öz nitelik seviyesi ve özellik seviyesi olmak üzere 3'e ayrılmaktadır. Testler sırasında ideal ışık ve hava durumu şartları kullanılmıştır. İlerleryan çalışmalarda daha zorlayıcı ortam şartları ile de bu çalışmanın genişletilmesi mümkündür.

Bryan ve diğ. [5] yaptığı çalışmada doppler radar izinden insan davranışlarının tanımlanması konusu ele alınmıştır. Bu çalışma sonucu geliştirilen SVM ile yürüme, koşma, dönme, yumruk atma, zıplama, oturma kalkma, sürünme ve ayakta durma hareketleri tanımlanmıştır. Alanda öncül olan bu çalışmanın daha da geliştirilmesi gerekliliği sonuçlar bölümünde vurgulanmıştır. Özellikle hareketlerin tamamen radara 90 derece karşıdan yapılması gerekliliği ve yatay alanda başarımın düşmesi yazarların en çok vurguladığı eksiklikler orarak ortaya çıkmaktadır.

Li ve diğ. [21] yaptığı çalışmada doppler radar sinyalleri ve giyilebilir bilekliklerin birlikte analizi üzerine çalışma yapılmıştır. Bu çalışma sonucu ortaya çift katmanlı Bi-LSTM ağı ile sensör füzyon tekniği geliştirilmiştir. Bu füzyon ile yapılan hareket analizlerinin başarımı yükseltilmiştir. Yürüme, ayakta durma, ayağa kalma, bir obje alma, ve su içme hareketleri

Severino ve diğ. [33] yaptığı çalışmada otomotivde kullanılan doppler radarlar üzerinde yaya tespit algoritmaları üzerine çalışılmıştır. Support Vektor Machine kullanılarak yapılan eğitim sonucunda arzulanan başarım oranları yakalanmıştır . Multi-Objective Optimizasyon teknikleri ile yapılan çalışmanın menzili ve kalitesi artırılmıştır. Fakat elde edilen sonuçlar istenen sonuca ulaşmasına rağmen gerçek zamanlı uygulamalar için fazla yavaş kalmıştır. Bu bakımdan çalışmanın daha da geliştirilmeye açık olduğu aşikardır.

Wang ve diğ. [44] yaptığı çalışmada milimetre dalga radar kullanılarak alınan sinyallerin kamera görüntüleri ile sensor füzyon yapılması üzerine çalışılmıştır. Burada alınan radar sinyallerinin ilgi alanları (reigion of interest) üzerine giydirilmesi ile oluşacak analizlerin doğruluğunun artırılması hedeflenmiştir.

Rodriguez ve diğ. [47] mikro doppler radarlar üzerine bir aldatma saldırısı gerçeklemişerdir. Bu alanda literatür taramamızda bulunan tek örnek bu saldırıdır. İlgili saldırıda insan tanımlamasını kardo vaskuler sistem özelliklerine dayanarak yapan sistemlere karşı insanın bu özelliğini taklit ederek saldırı gerçekleştirilmiştir.

Dave Tahmous ve Jerry Silvious [4] micro-doppler radarlarda Açı, Yükselti, Darbe Sıklığı (PRF-Pulse Repetation Frequency) ve Aydınlanmanın önemini araştırmışlardır. Bu araştırma ile birlikte hareketin radar bakışı ile olan açısının en önemli faktörlerden olduğunu göstermişlerdir.

Zabalsa ve diğ. [65] çalışmasında mikro doppler radarlar için bir sınıflandırma yöntemi önerilmektedir. Bu yöntem de STFT(Short time fourrier transform) edilen sinyalin zaman bağımlı ortalaması alınarak PCA (Pricipal Component Analysis) ile özellik çıkartımı yapılmaktadır. Yapılan özellik çıkartımının sonuda SVM (Support vektör machine) yardımı ile sınıflama yapılmaktadır.

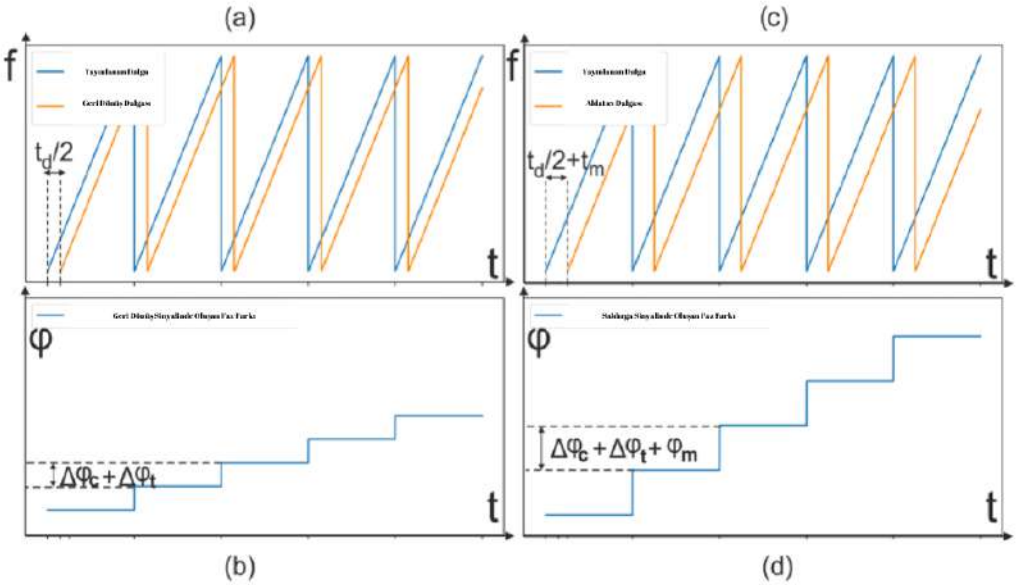
Yayın deneysel olması ve embedded sistemlerde çalışması bakımından önemlidir.

Arık ve diğ. [64] dairesel tabaka, kare tabaka ve kesik koni şekilinde hedeflerin radar üzerinde sınıflandırılması için Naive Bayes ve Yapay Sinir ağı temelli algoritmaların performanslarını karşılaştırmışardır. Yapılan karşılaştırmada NB temelli sınıflama için Gaussian, Üçgensel ve Epanechnikov çekirdekleri kullanılırken YS temelli sınıflandırmada Scaled Conjugate Gradient, Levenberg-Marquardt ve bayesian regulazition backpropagantion yöntemleri kullanılmıştır. Sonuç kısımında yazarlar en iyi sonucun YS temelli BRB algoritmasında olduğunu belirtmişlerdir.

Özellikle güvenlik alanında bu tip sensörlerin kullanımının yaygınlaşması ile birlikte bu tip sensörler üzerinde siber saldırıların artacağı öngörülebilirdir. Literatürde bu alanda yapılmış yayınların çok kısıtlı olduğu ve tek boyutlu olduğu gözlemlenmiştir [47]. Literatürde insan tanımlaması yapan sistemlere insanın araç veya hayvan gibi tanıtılması ile ilgili çalışma yapılmamıştır. Bu bakımdan İnsan tanımlaması yapılan sistemlerde yeni bir tip aldarma saldırısın geliştirilmesi gerekliliği gözlemlenmiştir.

Komissarov ve Wool'un [45] yaptığı çalışmada araç FMCW Radarlarına spoofing saldırısı düzenlenmekte ve bu saldırılara karşı güvenlik önlemleri de önerilmektedir . Bu saldırı için kurban aracın önüne geçen saldırgan araç arkasında bulunan SDR donanım aracılığıyla kurban aracın FMCW radarı sinyallerin manuple eder. Bu yolla gönderilen sinyaller aracılığıyla saldırgan aracın hızı ve iki araç arasındaki mesafe gibi kritik verilerin kurban araçda yanlış algılanması sağlanır. Deneysel çalışmada deneysel olarak gösterimi yapılan sistemde "bladeRF xA4" cihazı kullanılmıştır. Yapılan saldırının güncel üst düzey pek çok araçda bulunan FMCW sistemini ve dolayısıyla da ADAS (Advanced driver-assistance systems) sistemlerini hedeflemesi bakımından oldukça önemli olduğunu düşünmekteyiz. Makalenin son bölümünde saldırılara karşı önlem mekanizmaları da ele alınmıştır.

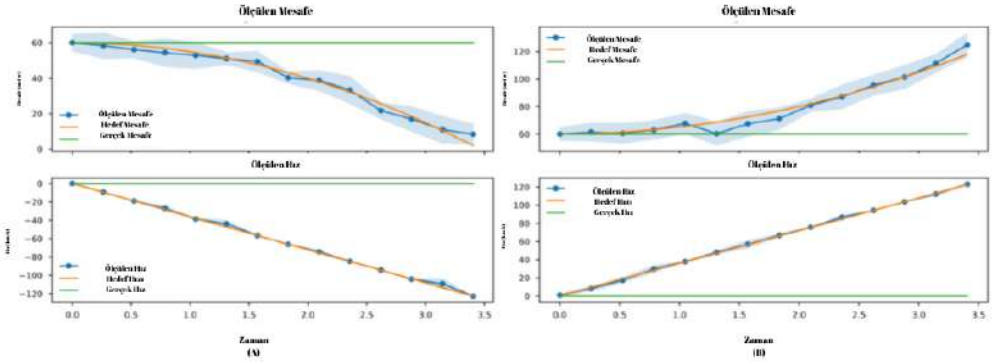
Öne sürülen 3 önlem mekanizması şu şekildedir; 1) [25]'de yapıldığı gibi kamera radar sensor füzyonu veya [46]'de yapılana benzer bir sensorfüzyon algoritması



Şekil 2.5: FMCW radar chrip sinyali ve saldırganın gerçekleştirdiği saldırı sinyali.

geliştirilmesidir. 2) Saldırılar donanımın faz farkı ölçüm mekanizmasına dayanmasından dolayı. Donanımsal geliştirmelerle rastgele faz kullanabilen radarların geliştirilmesi yönündedir. 3) [52] ve [49] önerildiği gibi frekans rastgele radarların geliştirilmesi. Bu sayede saldırgan doğru frekans düzeyinde saldırı sağlayamayacağı için saldırılar başarısız olacaktır. 4) Değişik hava durumlarına karşı dayanıksız bir yöntem olmakla birlikte dönüş sinyallerinde RSSI ölçümü yapmak da bir çözüm olarak önerilebilecek yöntemler arasındadır.

Brayan ve diğ. [5] UWB (Ultra Wide Band) radar kullanarak insan davranış sınıflandırması yapmışlarıdır. Yapılan deneysel çalışmalarda denekler yürüme, koşma, dönme, yumruk atma, zıplama, oturma-kalkma, sürünme, ve durmak gibi hareketleri yapmışlardır. Sinyal işleme aşamasında doppler radarların aksine UWB radarlar duran nesneleri ve yeri de algıladığı için öncelikle pre-process işleminden geçirilen data sonrasında PCA (Principal Component Analysis) 20 temel vektöre dönüştürülür. Bu vektörler SVM eğitiminde kullanılır ve sınıflandırma sağlanır. Çalışma alanında ilklerden olması ve UWB



Şekil 2.6: Saldırı sonucu oluşturulan hayalet objeler.

Radar kullanması açısında dikkate değerdir.

Nashimoto ve diğ. [48] FMCW radarlarına karşı spoofing saldırısı tasarlamışlardır. Tasarlanan saldırının amacı düşük maliyetli bir sistem yardımıyla FMCW radarında hayalet obje oluşturulabilmesi, radarın algıladığı mesafenin daraltılabilmesi idir. Bu çalışmada FMCW radarında spoofinge karşı önlemlerin mevcut olduğu var sayılmıştır (ECM- Electronic counter measure). Bu önlem rastgele zamanlı vuruş (chrip) kullanıldığı yönündedir. Bu önlemde dikkate alındığından önleme karşı önlem de (ECCM - Electronic counter counter measure) geliştirilmiştir. Karşı önlem olarak yapılan vuruşun önceden tahminlenmesi ve bu yolla saldırının yapılması sağlanmıştır. Sonuç olarak 10 Metre hata payı ile ilgili radarlarda saldırı gerçekleştirilebilmiştir. Bu sonuçların değerlendirilmesinde piyasada bulunan FMCW radarlarının ortalama menzilleri dikkate alınmamıştır. Bu noktanın da makalenin değerlendirmesinde dikkate alınması gerekir.

Yang ve Lv'nin [48] yaptığı çalışmada bağlı ve otonom araçlar (CAV-connected

and automated vehicles) için çeşitli sensor bazlı saldırılara karşı önlem mekanizması önerilmiştir. Bu önlem mekanizması temelinde artıklıka (reduncancy) dayanmaktadır. Tasarım hem araçta pekçok sensörün bulunması hem de pekçok aracın arasında sensör verisinin paylaşılmasını varsaymaktadır. Bu sayede pekçok sensorden alınan veriler geliştirilen H∞ bazlı algoritma sayesinde değerelendirilerek tekil sensorlerde oluşan hata veya saldırı durumları analiz edilmektedir. Böyle bir durum oluşması durumunda ilgili sensor görmezden gelinerek sistemin karar alması sağlanmaktadır. Bu sisteme dahil sensorlerin yarısından daha fazlası saldırıya uğramadığı durumlarda sistem stabilitesini koruyabilmektedir. Gelecekte yapılacak çalışmalarda senörlerin önemli bir kısımı saldırı altında olması durumu da ele alınabilir. Çalışma bu yönü ile geliştirilmeye açıktır.

Moon ve diğ. [49] FMCW radarlar için spoofing saldırılarına ve girişim durumlarına karşı gelişmiş yeni bir model önermektedirler. Bu model sayesinde saldırganların/diğer radarların hayalet obje oluşturma ihtimali ciddi oranda düşürülmektedir. Model rastgele frekans atlama (frequency random hooping) yöntemine dayanmaktadır. Standart FMCW radarlarının oluşturduğu gönderi (chrip) sinyali düzenli ve periyodik olmaktadır. BlueFMCW ile birlikte bu sinyalin LoRa sistemlerde [66]'de görülen rastgele gönderi metodolojisi ile gönderilmesi hedeflenmiştir. Bu rastgel gönderi sinyaline uygun olarak saldırgan sinyal üretmenin zorluğu nedeniyle hayalet objelere karşı direnç sağlanmaktadır. İlgili makale [49] ile birlikte önerilen metodun simulasyonlarla doğrulaması yapılmış olup ilerleyen aşamada deneysel çalışmalar yapılması mümkündür.

Sun ve diğ. [50] yaptığı çalışmada mmWave (Milimetre dalga radarları) radarlar üzerinde 2 saldırı yöntemi ve bunlara karşı savunma yöntemleri önerilmiştir. İlgili çalışmada önerilen yöntemler gerçeklenerek bir otonom araç üzerinde test edilmiştir. Deneyde ilgili otonom aracın karar alma mekanizmaları bu yolla kandırılılarak sistemin doğrulanması sağlanmıştır. Deneyler sırasında 5 senaryo denenmiştir. 1. senaryoda duran aracın önünde hayalet obje oluşturularak kırmızı ışıkta olan aracın geç hareket etmesi denenmiştir. 2. senaryoda hareketli araç önünde hayalet obje oluşturularak sert fren yapılması

ve bu yolla yolcuların tehtit edilmesi denenmiştir. 3. senaryoda ise hareketli araç önünde duran engel oluşturulması ve bu yolla kurban aracın şerit değiştirilmesi sağlanmıştır. 4. senayoda kurban araç önce önünde hayalet obje oluşturularak şerit değiştirmeye zorlanıyor 2. aşamada burada bulunan aracın konumu değiştirilerek otonom kurban aracın bu araca çarpması sağlanıyor. 5. senaryoda otonom olmayan kurban racın curise control sistemi saldırıya maruz bırakılarak oluşturulan hayalet obje yardımıyla ilgili aracın ani fren yapması sağlanıyor.

Li ve diğ. [21] doppler radar, accelormetre, jiroskop, ve manyetometreden alınan verilerle yürüme, oturma, ayağa kalkma, nesne alma, su içme, ve düşme olaylarını tanıyan algoritma geliştirmişlerdir. Sınıflandırmada accelormetre, jiroskop, ve manyetometreden alınan veriler tek bir IMU (internal measurment units) adı altında birleştirilirken radardan alınan veriler ayrıca değerlendirilmiştir. Makalenin ana konusu bu iki ana veri kaynağının deeplearning ile sensor füzyon yapılmasıdır.

Liu ve diğ. [18] pulse doppler radarların hareketli hedefleri dijital radyo frekansı hafızası (DRFM digital radio frequency memory) jammeri saldırısı altındayken tesbit edebilmesi için anit-velocity jamming stratejisi geliştirmişlerdir.

Li ve diğ. [67] FMCW radar ve doppler radarlar la gizli silah taşıma durumunun tespinin fizibilitesini incelemişlerdir. Bu çalışmada herhangi bir sınıflandırma yapılmamıştır. Sadece yürüme, gizli silah ile yürüme, kör bastonu ile yürüme, çanta ile yürüme ve kürek ile yürüme hareketleri yapılmıştır ve bu hareketlerin dopler radar izleri incelenmiştir. Çalışma sonunda bu şekilde bir sınıflandırmanın fizibil olduğu sonucuna ulaşılmıştır.

Saho ve diğ. [30] 24Ghz mikro doppler radar kullanarak kişi tanımlaması yapmışlardır. Bu çalışmada oturma ve kalkma hareketleri baz alınmıştır. Çalışma veri setinde 10 kişi kullanılmıştır bu bakımda veri seti geniş sahalarda uygulamalar için fizibilitenin ölçülmesi bakımından dar olarak kabul edilebilir. Fakat genel giriş çıkışın kısıtlı olduğu bakım evleri, özel tesisler gibi alnlarda kullanımı göstermek açısında yeterli kabul edilmelidir. Kullanılan sınıflama algoritması CNN dir.

Gürbüz ve diğ. [31] 5.8 Ghz Pulse doppler Radar, 10 Ghz CW Radar, 24 Ghz CW Radar, 40 kHz CW Sonar'ların yaşlı bakım evlerinde kullanımının fizibilitesini araştırmışlardır. Bu amaçla topallama, bastonla yürüme, yürüteçle yürüme ve tekerlekli sandalye ile hareketin sınıflandırılmasını yapmıştır. Yapılan çalışmada naive bayesian sınıflandırıcı kullanılmıştır. Sonuç olarak radar sistemlerinin menzil avantajının kapalı ortamlarda ortadan kalkması nedeniyle sonarların bu tip ortamlarda daha uygun labileceği değerlendirilmesi yapılmıştır. Yazarlar bu yönde ses dalgalarının hızı nedeniyle sonarın daha yüksek çözünülük elde etmesi, ortamın elektromanyetik gürültüsünden etkilenmemesi gibi faktörleri saymaktadır.

Sasakawa ve diğ. [68] insan tanıma için CW mikro dalga MIMO (Multiple input multiple output) radarların kullanımını araştırmıştır. Bu çalışmada etrafında pekçok radarın bulunduğu 8 kayıtlı denek ve 4 kayıtsız denek nefes alış verişleri üzerinden tanınmaya çalışılmıştır. Kullanılan radar ağının büyüklüğü ile başarım aoranının yükseldiğini gösteren çalışma 8X8 bir matrisin %100 başarım sağlayabildiğini iddia etmektedir.

Gao ve diğ. [32] araç üzerine FMCW radar yerleştirerek bir dizi deney yapmışlardır. Bu deneylerde park alanında, yolda sabit objeler ve yolcularla kayıt alınmıştır. Bu alınan kayılarla DT Baseline ve CDMC algoritmaları ile sınıflandırma yapılmıştır.

Zao ve diğ. [69] Paletli araçlar için CW Kara gözlem radarlarına karşı jammer geliştirmişlerdir. Paletlerin fiziksel geometrisine dayanan bu yöntem ile simulasyonlardan elde edilen sonuca göre yüksek kararlılıkta saldırgan sinyal üretilebilmiştir.

Fairchild ve Narayanan [70] yaptıkları çalışmada insan hareketlerinin sınıflandırılmasında iki farklı doppler radarın kullanımının fizibilitesini araştırmışlardır. Kullanılan s-band ve mmDalga radarlarının her ikiside yüksek doğrulukla nefes alma, kolları sallama, yerden nesne alma, ve ayağa kalkma hareketlerini bir duvar arkasından yüksek başarımla sınıflayabilmişlerdir. Bu sınıflama esnasında mmDalga radar daha başarılı olmuştur.

Sang ve Kang [71] SFSK ve FSA radar sinyalleri üzerinden duran insanın tespit edilmesi üzerine çalışmışlardır. Bu çalışmada inasnın nefes alma hareketleri değerlendirilerek duran insanların tesbit edilebileceğini gösterilmiştir.

Fioranelli ve diğ. [16] inek ve koyunlarda toplallık tespiti için FMCW radar kullanılması için çalışmışlardır. Bu makalede 51 inek ve 75 koyun için deneysel olarak yapılan doğrulama çalışmasının ineklerde %80 koyunlarda ise %90 oranında doğru sınıflama yapılabildiğine değinilmektedir. Kullanılan 2 sınıflandırma algoritmalarından KNN daha zayıf kalırken önceki cümlede belirtilen sonuçlara Naive Bayes sınıflandırıcı ile ulaşılmıştır.

İslam ve diğ. [27] 2.4Ghz doppler radarlar kullanarak insan nefes alışverişlerini ve kalp atışlarını yakalamaya çalışmıştır. SVM ile sınıflandırma çalışması gerçek değere %92 doğrulukta benzerlik göstermektedir.

Ilioudis ve diğ. [72] mikro insansız hava araçlarının öz savunması için bir jammer (ECM) geliştirlmesi üzerine çalışmışlardır. POFACETS temelli ve matamatik modellere dayanan simulasyonlarda bu ECM'nin fizibilitesi gösterilmiştir.

2.5. İLETİŞİM KANALLARINDA DOS SALDIRILARININ TESPİTİ

Boche ve diğ. [73], haberleşme sistemleri bağlamında, fiziksel bir kanalın sıkıştırılıp sıkıştırılmadığının algoritmik olarak anlaşılmasının mümkün olmadığını göstermiştir. Şöyle ki, bir iletişim kanalında karıştırıcının tespiti prensipte algoritmik olarak her durumda gerçekleştirilemez. Örneğin, $F(W) = 0$ olduğunda, bir DoS saldırısının mümkün olup olmadığını belirlemek için durdurma probleminin çözülesi gerekmektedir.

Durdurma Problemi, bir bilgisayar programının belirli bir giriş için sonlu bir sürede durup durmayacağını belirlemenin imkansız olduğunu ifade eden bir problemdir. Bu problem, Turing tarafından çözülmez olarak kanıtlanmıştır ve algoritmik olarak belirlenemez.

Kanal Tanımı

$$W : X \times S \to P(Y) \tag{2.7}$$

Burada X giriş alfabesini, S karıştırıcı durumlarını ve Y ise çıkış alfabesini temsil eder.

Ortalama Kanal Kapasitesi Karıştırıcının belirli bir $q \in P(S)$ dağılımını seçmesi durumunda, ortalama kanal aşağıdaki gibi tanımlanır:

$$W_q(y|x) := \sum_{s \in S} W(y|x,s)q(s) \tag{2.8}$$

Burada $x \in X$, $y \in Y$ ve $q(s)$ karıştırıcı durumunun olasılık dağılımıdır.

Kapasite Tanımı

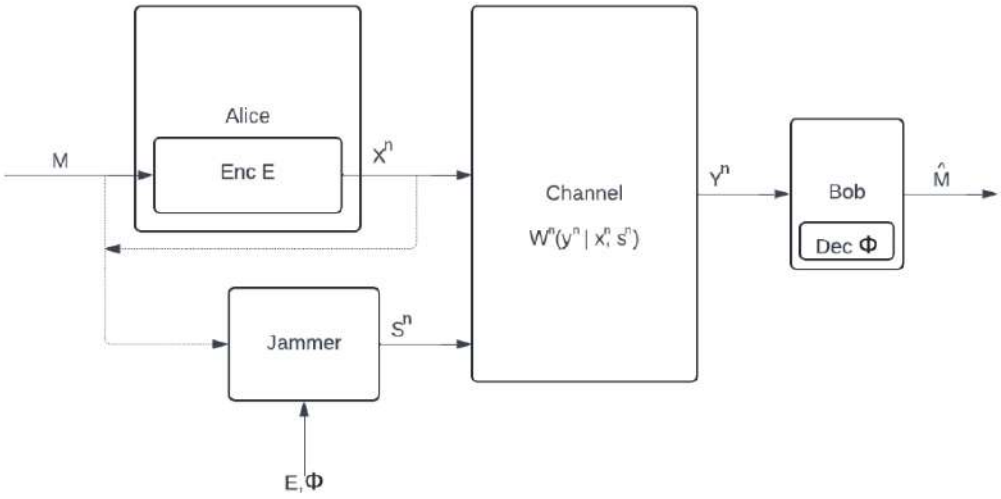
$$C(W) = \begin{cases} \min_{q \in P(S)} C(W_q) & \text{eğer } F(W) > 0 \\ 0 & \text{eğer } F(W) = 0 \end{cases} \tag{2.9}$$

Burada $F(W)$ simetrizasyon fonksiyonudur ve aşağıdaki gibi tanımlanır:

$$F(W) = \min_{U \in CH(X;S)} \max_{x \neq x'} \sum_{y \in Y} \left| \sum_{s \in S} W(y|x,s)U(s|x') - \sum_{s \in S} W(y|x',s)U(s|x) \right| \tag{2.10}$$

Eğer $F(W) = 0$ ise, bu durum kanalın simetrik olduğunu ve bir DoS saldırısının mümkün olduğunu gösterir. Bu senaryoda, kanal kapasitesi $C(W) = 0$ olacaktır.

Bir iletişim kanalında, sinyallerin gürültüden mi yoksa kasıtlı bir karıştırmadan mı kaynaklandığını belirlemek için bir algoritma geliştirmek, aynı şekilde imkansızdır. **Şekil 2.7**'de gösterilen sistemle çalışan bir karıştırıcının, geçerli sinyalin üstüne bir gürültü ekleyerek veya sinyali değiştirerek iletişimi kesintiye uğratabilir. Ancak, bu kesintinin bir karıştırıcıdan mı yoksa doğal bir gürültüden mi kaynaklandığını belirlemek için tüm olası gelen sinyal ve gürültünün hesaplanması gerekmektedir. Bu da



Şekil 2.7: Bochenin çalışmasında jammerin çalışma mekanizması.

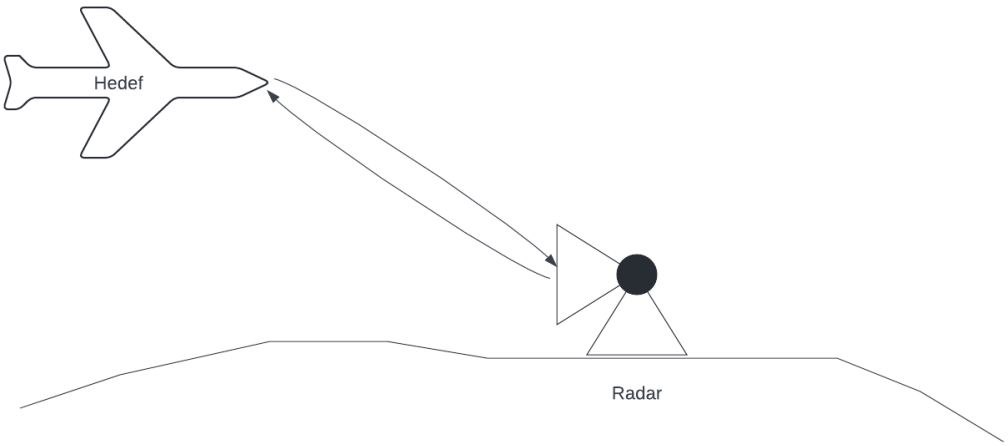
durdurma probleminde olduğu gibi bir öz döngüye girlimesine yol açacaktır ki bu problem, algoritmik olarak çözülemeyen bir problemdir.

Bu nedenle, bir iletişim kanalında karıştırma tespitinin algoritmik olarak belirlenemeyeceği sonucuna varılır. Durdurma Problemi gibi, bu problem de herhangi bir genel çözümle belirlenemez; bu nedenle, karıştırma tespiti için algoritmik bir çözüm mümkün değildir.

2.6. RADARLARDA DOS SALDIRILARININ TESPİTİ

Radarların çalışma prensibine bakıldığında, belirli bir kanalda radyo frekansı yayını yaparlar ve hedeften döndüklerinde veri üretirler. Bu açıdan, radar sensör kanallarının analog haberleşme kanalları olarak düşünülmesi doğaldır. Yukarıdakilerden anlaşılacağı üzere, radar sistemlerinde bir kanalda sıkıştırma saldırısı olup olmadığını algoritmik olarak anlamak imkansızdır.

Bu tezde, mikro doppler radar temelli insan-hayvan ayrımı yapan sistemler



Şekil 2.8: Radar algılaması iletişim kanalı benzerliği.

üzerinde yoğunlaşılmıştır. Bu sistemlerin temelinde yatan teori aşağıdaki şekilde özetlenebilir:

- Tüm radar tipleri, çalışma prensibi itibariyle bir sinyal yayınlamakta ve bu sinyalin geri dönüşüne bakarak hedefleri tespit ve teşhis etmektedirler. Bu bağlamda, radar ile hedef tespiti, karşılıklı yayın yapan iki ögenin iletişim kurduğu bir iletişim kanalı ile eşlenik bir değere sahiptir.
- Boche ve diğ. [73] gösterdiği üzere, bir iletişim kanalında jamming yapılıp yapılmadığının algoritmik olarak anlaşılması imkansızdır. Çünkü ilgili problem durdurma problemi ile eşlenik bir problemdir. Dolayısıyla, radar ile hedef tespit ve teşhis işlemi gerçekleştirildiğinde, bu sürecin karıştırma veya aldatma saldırısı altında olup olmadığının algoritmik olarak tespiti mümkün değildir.
- Halting problemi ile eşlenik problemlerin sezgisel yöntemlerle çözülmesi mümkündür [74, 75]. Bu nedenle, radar sistemlerinde karıştırma veya aldatma saldırılarının anlaşılması için sezgisel yöntemlerin kullanılması mümkündür.

Bu teoriyi deneysel olarak ispatlamak amacıyla, mikro doppler radar temelli insan-hayvan sınıflandırması yapan bir sistem geliştirilmiş ve bu sisteme yönelik bir karıştırma saldırısı gerçekleştirilmiştir. Yapılan karıştırma

saldırısını tespit ve teşhis etmek için çeşitli mekanizmalar geliştirilmiştir. Bu tür bir saldırı altında çalışabilmesi için insan-hayvan ayrım mekanizmaları güncellenmiş ve karşı önlem mekanizmaları tasarlanmıştır. Bu süreç ve kullanılan yöntemler, Malzeme ve Yöntem bölümünde detaylı olarak açıklanacaktır.

3. YÖNTEM

Tez kapsamında istenilen ölçütlere uygun örnek bir aktif radar sistemi ve karıştırma sisteminin birlikte bulunduğu bir veri seti görülememiştir. İsrail ordusunun yayınladığı MAFAT veri [76] Veri seti içerisinde radar ve insan verilerinin bir arada bulunduğu bir set olarak görülmektedir. Fakat bu veri seti içerisinde jammer verisi bulunmamaktadır. Ayrıca askeri tip pulse doppler radarlar kullanılmaktadır. Dolayısıyla bu çalışma kapsamı ile doğrudan ilişkili sayılmamalıdır. Bu bakımdan tezin deneysel aşamalarının tamamlanması için baştan bir veri seti elde edilmesi büyük önem arz etmektedir. Oluşturulacak bu tip bir veri seti sayesinde ilerleyen yıllarda da yeni araştırmaların yapılabilecek olması veri setinin kıymetini artıran unsurlardan birisi olarak da sayılabilir. Bu nedenle gerekli deneylerin tüm parçaları özel olarak üretilmiştir.

- Öncelikle uygun bir veri seti tasarlanmışıtır.
- Bu veri setini uygun olarak toplayabilecek bir cihaz tasarlanımış ve gerçeklenmiştir.
- Bu cihazla birlikte veri seti toplanmıştır.
- Toplanan veri seti ile klasik bir analiz yöntemi gerçeklenmiştir.
- Yeni bir radar saldırı yöntemi gerçeklenmiştir.
- Saldırı yönteminin başarımı ölçülerek bir referans noktası oluşturulmuştur .
- Saldırı yöntemine karşı dirençli yeni bir yapay zekanın eğitilmiştir.
- Yeni saldırı direnç yönteminin başarımı ölçülmüştür.

3.1. VERİ SETİ OLUŞTURULMASI

Literatürde incelenen çalışmalar ışığında, belirli durumlarda ayrım yapabilen bir doppler radar sisteminin geliştirilmesi amaçlanmıştır. Bu bağlamda, aşağıdaki senaryolarda veri toplanmasına karar verilmiştir:

1. **İnsan Yürüyüşü:**

   İnsan yürüyüşü, radar sisteminin en temel insan hareketlerini algılama ve sınıflandırma kabiliyetini değerlendirmek için kritik bir senaryodur. Bu veri, sistemin normal insan hareketlerini doğru bir şekilde tanımlayabilmesi için gereklidir.

2. **İnsan Sürünme:**

   Sürünme hareketi, standart yürüme ve koşma hareketlerinden farklı dinamiklere sahiptir. Bu senaryonun eklenmesi, sistemin farklı insan hareketlerini ayırt etme ve potansiyel gizli girişimleri tespit etme yeteneğini artırır.

3. **İnsan Zıplama:**

   Zıplama hareketleri, radar sinyallerinde farklı yansımalar oluşturarak sistemin dikey hareketleri algılama kabiliyetini test eder. Bu, sistemin çeşitli insan aktivitelerini sınıflandırmasında önemli bir rol oynar.

4. **İnsan Metal Sopa İle Yürüme:**

   Metal bir nesne ile yürüyen insan verileri, radar sinyallerindeki metal yansımalardan kaynaklanan değişiklikleri anlamak için kullanılır. Bu, güvenlik uygulamalarında tehlikeli nesnelerin tespitine katkı sağlar.

5. **İnsan Koşma:**

   Koşma hareketi, daha yüksek hız ve farklı hareket dinamikleri içerir. Bu veri, sistemin hızlı hareket eden insanları doğru bir şekilde algılamasını ve sınıflandırmasını sağlar.

6. **Köpek Koşma:**

   Köpeklerin koşma hareketleri, hayvan ve insan hareketleri arasındaki

farkları belirlemek için önemlidir. Bu, sistemin insan olmayan hedefleri doğru bir şekilde sınıflandırmasına yardımcı olur.

7. **Köpek Durma:**

   Köpeğin durma ve minimal hareket etme durumları, radar sisteminin düşük hareket aktivitelerini algılama hassasiyetini değerlendirmek için kullanılır.

8. **At Dolaşma:**

   Atların dolaşma hareketleri, büyük hayvanların radar imzalarını anlamak için kritiktir. Bu veri, sistemin farklı boyutlardaki hayvanları ayırt etme kabiliyetini artırır.

9. **At Biniciliği:**

   At üzerinde insan hareketleri, hem insan hem de hayvan hareketlerinin birleşik etkisini incelemek için eklenmiştir. Bu, karmaşık hedeflerin algılanmasında sistemin performansını değerlendirir.

10. **Eşek Dolaşma:**

    Eşeklerin hareketleri, benzer boyut ve hareket özelliklerine sahip hayvanların sınıflandırılmasında kullanılır. Bu, sistemin hassasiyetini ve doğruluğunu artırır.

11. **Eşek Biniciliği:**

    Eşek üzerinde insan hareketleri, yine birleşik hareketleri incelemek ve sistemin bu tür senaryolarda performansını test etmek için önemlidir.

12. **İnek:**

    İneklerin hareketleri, büyük ve yavaş hareket eden hayvanların radar imzalarını elde etmek için kullanılır. Bu, tarım ve kırsal alan uygulamaları için değerlidir.

13. **Geyik:**

    Geyik verileri, vahşi hayvanların hızlı ve ani hareketlerini anlamak

için önemlidir. Bu, özellikle ormanlık ve doğal yaşam alanlarındaki uygulamalarda sistemin etkinliğini artırır.

14. **Koyun:**

    Koyun sürülerinin hareketleri, grup halinde hareket eden küçük hayvanların sınıflandırılmasına yardımcı olur. Bu, sürü davranışlarının anlaşılması için önemlidir.

15. **Tavuk:**

    Tavuklar, küçük ve hızlı hareket eden hayvanlardır. Bu veriler, sistemin küçük hedefleri algılama ve sınıflandırma kabiliyetini değerlendirir.

İlk tasarım aşamasında, bu senaryoların her biri için 0, 5, 10, 15 ve 20 metre mesafelerde veri toplanması ve bu verilerin 90°, 60°, 30° ve 0° açılardan elde edilmesi planlanmıştır. Her bir senaryo için beş farklı denek kullanılarak, her denekten 20 kayıt alınması durumunda, senaryo başına her bir veri tipi için 2.000 kayıt elde edilmesi hedeflenmiştir. Bu şekilde, veri setinde toplamda 30.000 sn kayıt yapılması amaçlanmaktadır.

Bu kapsamlı veri toplama stratejisi, sistemin farklı mesafe ve açı koşullarında performansını değerlendirmeyi ve çeşitli hareket senaryolarında yüksek doğrulukla sınıflandırma yapabilmesini sağlamayı hedeflemektedir.

Ancak, teknik imkanlar dahilinde bu şekilde bir veri setinin toplanmasının zor olduğu anlaşılmıştır. Özellikle, vahşi hayvanların (örneğin geyik) istenilen açılarda istenilen yönlerde radarlara yaklaşmasının sağlanmasının neredeyse imkansız olduğu anlaşılmıştır. Ayrıca bu hayvanların doğal davranış patternlerini de bu şekilde yansıtmanın doğru olmayacağı da düşünülmektedir. Vahşi hayvanların davranışlarının daha sürü davranışı olması ve kaotik olması nedeniyle bu şekilde bir veri toplanmasının daha doğru olacağı düşünülmektedir.Bu sebeple, veri seti yeniden tasarlanarak daha kaotik bir yapıya izin verilmiştir. Değişik açılar ve mesafeler gibi ayrımlar ortadan kaldırılarak, veri toplama süreci daha esnek hale getirilmiştir. Genel olarak hayvanların radar çevresinde serbest olarak dolaşması sağlanmıştır. Bu şekilde, algoritmanın eğitim başarısının biraz düşebileceği kabul edilmekle birlikte,

gerçek hayatta uygulandığında daha yüksek bir performans elde edileceği öngörülmektedir. Çünkü gerçek dünyada, insan ve hayvan davranışlarının zaman zaman öngörülebilir olmasına rağmen, tam anlamıyla kontrol edilmesi oldukça zor olacaktır. Bu durumda, daha kaotik bir veri setinin, algoritmanın genel dayanıklılığını artırabileceği düşünülmektedir. Yeniden tasarlanan veri seti için belirlenen senaryolar aşağıdaki gibidir:

Şekil 3.1: Veri toplanması esnasında geyikler.

1. **İnsan Yürüyüşü:**

   İnsan yürüyüşü verileri, insan hareketinin en temel biçimlerinden birini temsil etmektedir. Bu veriler, sistemin insan hareketini doğru bir şekilde tanımlaması ve sahtekarlık girişimlerini tespit etmesi açısından kritik öneme sahiptir.

2. **İnsan Koşma:**

   Koşma hareketi, yürüme hareketinden farklı dinamiklere sahiptir. Bu veriler, sistemin farklı hızlardaki insan hareketlerini doğru bir şekilde sınıflandırmasını sağlamaktadır.

Şekil 3.2: Veri toplanması esnasında kurt.

3. **İnsan Grup Yürüme:**

   Grup halinde yürüyen insanların verileri, radar sisteminin birden fazla hedefi ayırt edebilme yeteneğini test etmektedir. Bu, kalabalık ortamlarda veya birden fazla insanın bulunduğu senaryolarda sistemin etkinliğini değerlendirmek için değerlidir. Özellikle kullanılan vahşi hayvanların sürü halinde dolaşması nedeniyle bu kalabalık hareketin insanlarla birlikte de tekrar edilmesi gerçek hayat davranışının doğru simule edilmesi için kritik önem arz etmektedir.

4. **İnsan Metal Sopa İle Yürüme:**

   Metal bir nesne ile yürüyen insan verileri, radar sinyallerinde farklı yansımalar oluşturarak sistemin metal nesneleri algılama ve sınıflandırma yeteneğini test etmektedir. Bu, güvenlik uygulamaları için önemli bir özelliktir.

5. **İnsan Metal Sopa İle Koşma:**

Metal bir nesne ile koşan insan verileri, hem yüksek hızda hareketin hem de metal nesnelerin radar üzerindeki etkisini incelemek için kullanılır. Bu, sistemin dinamik ve karmaşık senaryolarda performansını değerlendirmeye yardımcı olur.

6. **At Dolaşması:**

   Atların hareketleri, büyük hayvan hareketlerinin radar imzalarını anlamak için önemlidir. Bu veriler, sistemin farklı boyutlardaki hayvanları tanımlama kabiliyetini geliştirmektedir.

7. **Geyik Dolaşması:**

   Geyik verileri, vahşi hayvan hareketlerinin radar imzalarını elde etmek için önemlidir. Bu, özellikle ormanlık alanlardaki uygulamalar için değerlidir. **Şekil 3.1**'de veri toplaması esnasında geyiklerin fotoğrafı mevcuttur.

8. **Koyun Dolaşması:**

   Koyun hareketleri, sürü davranışlarını ve küçük hayvan hareketlerini anlamak için toplanmıştır. Bu, sistemin farklı hayvan türlerini ayırt etme yeteneğini geliştirir.

9. **Cüce Domuz Dolaşması:**

   Cüce domuz verileri, küçük ve orta boy hayvanların radar imzalarını elde etmek için önemlidir. Bu, sistemin çeşitli hayvan boyutlarını tanımasını sağlar.

10. **Kurt Dolaşması:**

    Kurt hareketleri, yırtıcı hayvanların dinamiklerini anlamak için toplanmıştır. Bu, güvenlik ve vahşi yaşam izleme uygulamalarında kritiktir.

11. **Ceylan Dolaşması:**

    Ceylan verileri, hızlı hareket eden hayvanların radar imzalarını elde etmek için değerlidir. Bu, sistemin yüksek hızlı hedefleri izleme kabiliyetini artırır.

12. **Keçi Dolaşması:**

    Keçi hareketleri, dağlık ve engebeli arazilerdeki hayvan hareketlerini anlamak için önemlidir. Bu veriler, sistemin çeşitli çevresel koşullarda performansını değerlendirmeye yardımcı olur.

13. **Hedef Olmadan Boş Kayıt:**

    Boş kayıtlar, radar algılama alanında herhangi bir hedefin bulunmadığı durumları temsil eder. Bu veriler, sistemin gürültü ve çevresel faktörlere karşı duyarlılığını değerlendirmek ve yanlış alarm oranlarını azaltmak için kullanılır.

14. **Çok Yakından El Sallayarak Gürültü Oluşturma:**

    Radar antenine çok yakın mesafede el sallayarak oluşturulan gürültü verileri, sistemin yakın mesafede oluşabilecek parazitlere ve karıştırma girişimlerine karşı tepkisini test etmek için önemlidir. Bu, sistemin güvenilirliğini ve karıştırma saldırılarına karşı dirençliliğini artırmaya yardımcı olur.

Bu senaryolar kapsamında, veri setinin daha gerçekçi ve uygulamaya yönelik hale getirilmesi hedeflenmiştir. Bu durum, veri setinin algoritma eğitimine sunduğu katkıyı artırarak, gelecekteki uygulamalarda daha başarılı sonuçlar elde edilmesini sağlayabilir.

3.1.1. Veri Toplama Cihazının Oluşturulması

Veri toplama cihazı tasarlanırken birkaç kriter göz önüne alınmıştır. Bunlar kolay bir şekilde gerçeklenebilmesi, vahşi hayat ortamında veri toplama yapılacağı için enerji etkinliğinin olması, hayvanların doğal davranabilmesi için dikkati çok çekmemesi gerekmektedir dolayısıyla, fiziksel olarak küçük olması da bir kiriterdir. Sayılan kirterlere göre seçilebilecek radar tipleri ve bununla ilgili toplanacak verinin niteliği aşağıda detaylandırılmaktadır:

Sürekli Dalga Doppler Radarı Sürekli olarak belirli bir frekansta yayın yapan bu radar tipi, geri dönüş dalgasında oluşan frekans farkına uygun

olarak çıkış sinyali üretmektedir. Çıkış sinyali büyük oranda doppler etkisine dayanmaktadır. Doppler etkisi hedefe çarpan radyo dalganın hedefin hızına göre frekans değiştirmesi prensibine dayanmaktadır. Hareket eden hedef sinyali geri yansıtırken oluşan doppler etkisi sinyali oluşturmaktadır. Elde edilen bu sinyalden hedefin hızı hakkında bilgi alınmaktadır. Tahmous ve Silvious'un [1] çalışmalarında da gösterildiği gibi, insan yürüyüş izinde bacak, kol, gövde gibi vücut parçalarının ayrımı yapılabilmektedir. Literatürde taranan 33 yayından 21'inde sürekli dalga doppler radarı kullanıldığı görülmüştür.

Vuru Dalga Radarı Bu radar tipi, belirli aralıklarla vuru (pulse) üretir ve bu vurunun geri dönüş zamanına göre çıkış sinyali oluşturur. Bu sinyalde, hedefin uzaklığına dair bilgi bulunmaktadır. Ancak, bu tip radarların gerçekleştirilmesi için gerekli elektronik donanım nispeten karmaşık olduğundan, yaygın olarak tercih edilmemektedir. Taranan 33 yayından yalnızca 2'sinde Vuru Dalga Radarı kullanılmıştır.

Vuru Dalga Doppler Radarı Vuru Dalga Radarı ile benzer özellikler taşıyan bu radar tipi, vurunun dönüş zamanı dışında dönüşteki frekans farkını da ölçerek çıkış sinyalinde hem mesafe hem de hız bilgilerini aynı anda sağlamaktadır. Ancak, taranan 33 yayından hiçbirinde vuru dalga doppler Radarı kullanılmadığı tespit edilmiştir.

Frekans Düzenlenmiş Sürekli Dalga Radarı Bu radar tipi, sabit bir frekansta değil, düzenlenmiş bir frekansta çıkış sinyali üretmektedir. Bu sayede, hedefin hızıyla birlikte mesafesi de ölçülebilmektedir. Literatürde taranan 33 yayından 10'unda Frekans Düzenlenmiş Sürekli Dalga Radarı kullanıldığı görülmüştür.

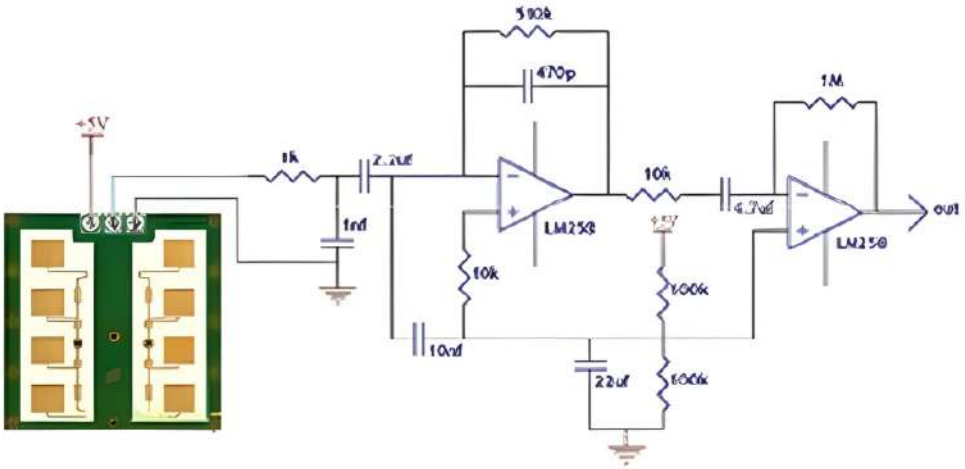
Bu radar tiplerinin her biri, farklı veri toplama senaryoları için belirli avantajlar sunmakta ve bu çalışmada hedeflenen insan sınıflandırma ve sahtecilik tespiti amacı doğrultusunda uygun radar tipinin seçilmesi kritik öneme sahiptir.

Literatürde mevcut sistemlerin çoğunluğunda CW (Sürekli Dalga) tipi doppler radarlarının kullanıldığı göz önünde bulundurularak, bu çalışmada da sistemin CW doppler radarlar ile gerçekleştirilmesine karar verilmiştir. CW doppler

radarlarının tercih edilmesinin başlıca nedenleri arasında düşük güç tüketimi, basit yapısı ve güvenilir performansı gibi özellikler bulunmaktadır.

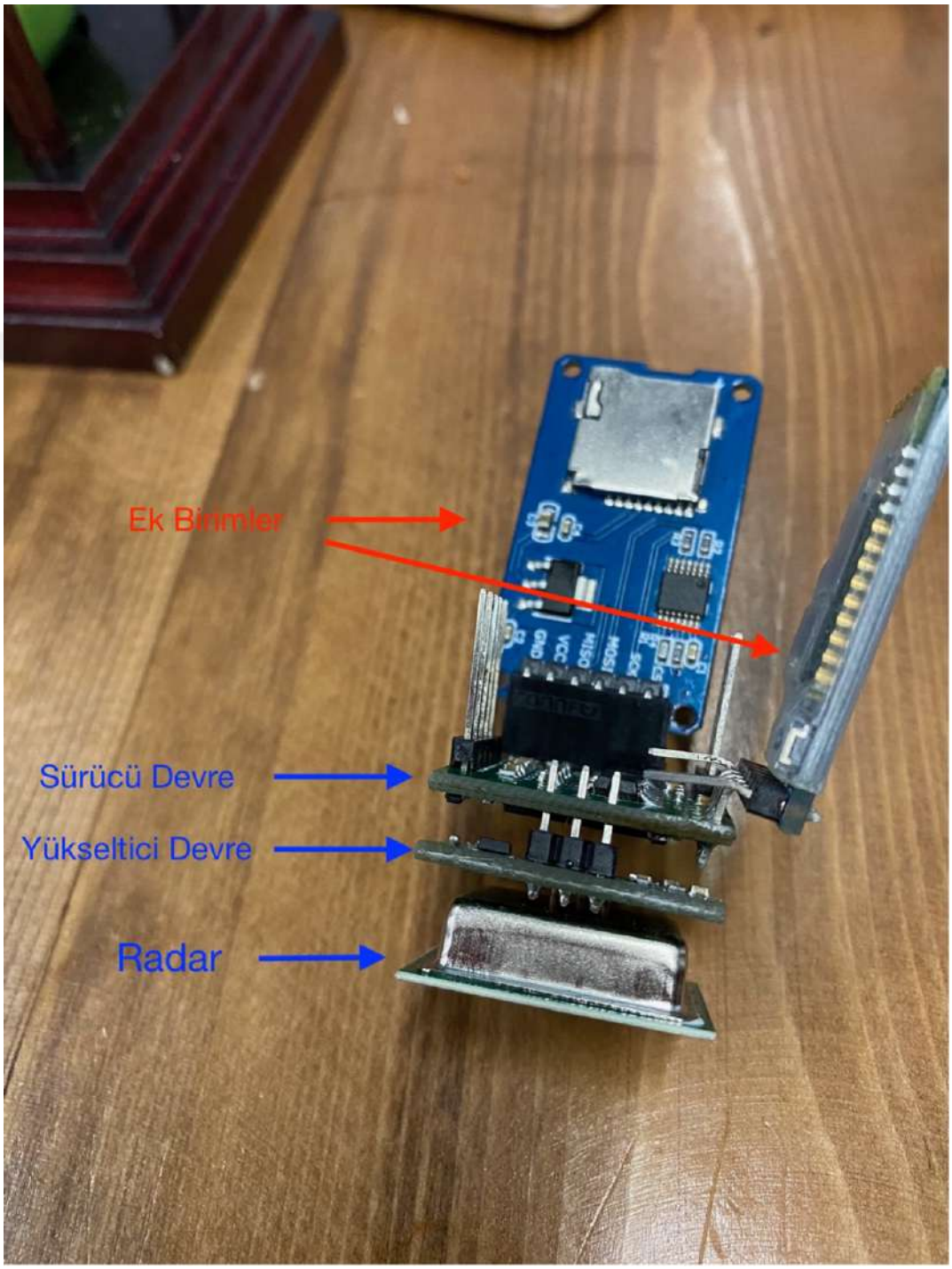
Piyasada bulunan mikro doppler radarlar değerlendirilmiş ve bu radarlar arasından en uzun menzile sahip olan CDM324 sisteminin kullanılması uygun görülmüştür. CDM324, referans yükseltici devre ile birlikte 15 metre menzilli olarak tasarlanmıştır. Bu referans devresinin sinyal güçlendirme oranı 51,000 olarak belirlenmiştir. Ancak, yeni tasarlanan güçlendirici devre ile bu oran 100,000 katına çıkarılmıştır. Bu sayede, 20 metre civarındaki bir menzil için tasarlanan sistemin yeterli algılama kapasitesine sahip olması hedeflenmiştir.

Bu tasarım yaklaşımı, radar sisteminin geniş bir menzil aralığında güvenilir veri toplamasını sağlamayı amaçlamaktadır. Böylece, doppler radar tabanlı insan sınıflandırma sistemlerinde kullanılacak verilerin doğruluğu ve güvenilirliği artırılacaktır. Ayrıca, CW doppler radarların sahip olduğu düşük güç tüketimi ve basit yapı, sistemin taşınabilirliği ve uzun süreli saha kullanımına da katkıda bulunacaktır.



Şekil 3.3: CDM324 ve referans devresi

Sistemin sürücü devresi STM32F373GMT entegresi temelinde kurgulanmıştır. İlgili entegrenin 16bit SDADC bulundurması veri kalitesini olumlu etkileyecek bir faktör olarak değerlendirilmektedir.



Şekil 3.4: Veri toplama cihazı

3.1.2. Veri Seti Toplanması

Bu çalışmada, doppler radar tabanlı insan sınıflandırma sistemlerinde yapılacak sahtecilik saldırılarına yönelik olarak farklı mesafelerde ve açılarda veri toplanması planlanmıştır. Spesifik olarak, 0, 5, 10, 15 ve 20 metre mesafelerde veri toplanacak olup, bu mesafelerdeki sinyaller 90, 60, 30 ve 0 derecelik açılardan elde edilecektir. Her bir senaryo için beş farklı denek kullanılarak, her denek için 20 kayıt alınması hedeflenmiştir. Bu şekilde, senaryo başına toplam 2,000 kayıt elde edilmesi ve nihai veri setinde toplamda 40,000 kayda ulaşılması amaçlanmıştır.

Ancak, bu veri toplama süreci sırasında bazı zorluklarla karşılaşılmıştır. Örneğin, vahşi hayvanların varlığı ve evcil hayvanların belirli açılarda ve limitlerde algılanmasındaki zorluklar, bu kadar detaylı bir veri toplama sürecini imkânsız hale getirmiştir. Özellikle geyik ve domuz gibi hayvanların genellikle sürüler halinde dolaşması, toplanacak verilerin gerçekçiliğini azaltmaktadır. Bu nedenle, verilerin serbest dolaşma tekniği ile toplanmasına karar verilmiştir.

Sonuç olarak, insan yürüyüşü, insan zıplaması, metal sopa ile yürüme, insan koşması, köpek koşması, at dolaşması, eşek dolaşması, geyik, koyun, metal sopa ile koşu, cüce domuz, kurt, ceylan, keçi, boş kayıt ve aşırı yakın hedef olmak üzere 12 farklı senaryo için toplamda 3,745 saniyelik kayıt elde edilmiştir. Bu kayıtlar, her biri 12,5 milisaniye süren bölütlere ayrıldığında, 299,600 ayrık kayıt elde edilmiştir.

Bu veri seti, doppler radar tabanlı insan sınıflandırma sistemlerine yönelik sahtecilik saldırılarını tespit etmek ve bu tür sistemlerin güvenliğini artırmak amacıyla kullanılacaktır. Ayrıca, farklı senaryolar altında elde edilen bu kapsamlı veri seti, ileriye dönük çalışmalar için de önemli bir kaynak sağlayacaktır.

3.2. KLASİK ANALİZ YÖNTEMİNİN GERÇEKLEŞTİRİLMESİ

Klasik analiz yöntemlerinin performansını değerlendirmek amacıyla, Matlab programında bulunan *Classification Learner* aracı kullanılarak çeşitli modeller eş zamanlı olarak gerçekleştirilmiştir. Bu süreçte, farklı makine öğrenimi algoritmaları arasında karşılaştırmalar yapılmış ve en yüksek doğruluk oranına sahip modeller belirlenmiştir. Yapılan analizler sonucunda, *Ensemble Bagged Trees* ve *Fine Gaussian SVM* modelleri en yüksek başarıma sahip yöntemler olarak öne çıkmıştır.

Ensemble Bagged Trees modeli, birden fazla karar ağacını kullanarak tahminlerin doğruluğunu artırmayı amaçlayan bir yöntemdir. Bu model, veriyi farklı alt kümelere ayırarak her bir alt küme üzerinde ayrı ayrı eğitim gerçekleştirir ve ardından bu tahminlerin ortalamasını alarak nihai tahmini oluşturur. Bu yaklaşım, özellikle karmaşık veri setlerinde modelin genelleme kabiliyetini artırarak daha doğru sonuçlar elde edilmesini sağlar.

Ensemble Bagged Trees modelinin matematiksel temeli, birden fazla karar ağacının bir araya getirilmesine dayanır. Bu model, bootstrap aggregating (bagging) tekniğini kullanarak veri setinden rastgele örnekler seçer ve her bir örnek üzerinde ayrı bir karar ağacı eğitir. Modelin genel formülasyonu şu şekildedir:

$$\hat{f}_{bag}(x) = \frac{1}{B}\sum_{b=1}^{B} \hat{f}^{*b}(x) \tag{3.1}$$

Burada:

- $\hat{f}_{bag}(x)$: Bagged trees modelinin nihai tahmini
- B: Toplam ağaç sayısı
- $\hat{f}^{*b}(x)$: b. ağacın tahmini

Her bir ağaç, orijinal veri setinden bootstrap örnekleme ile oluşturulan farklı bir

eğitim seti kullanılarak oluşturulur. Bootstrap örnekleme, n boyutlu orijinal veri setinden n boyutlu yeni bir veri seti oluşturmak için rastgele örnekleme (yerine koyarak) yapılmasıdır.

Bagged trees modelinin varyansı şu şekilde hesaplanır:

$$Var(\hat{f}_{bag}(x)) = \rho\sigma^2 + \frac{1-\rho}{B}\sigma^2 \tag{3.2}$$

Burada:

- ρ: Ağaçlar arasındaki ortalama korelasyon
- σ^2: Tek bir ağacın varyansı

Bu formülasyon, bagged trees modelinin, özellikle ağaçlar arasındaki korelasyon düşük olduğunda ve ağaç sayısı (B) arttıkça varyansı azalttığını göstermektedir.

Fine Gaussian SVM ise, sınıflandırma problemlerinde kullanılan bir destek vektör makinesi (SVM) modelidir. Bu model, veriyi sınıflar arasında en iyi şekilde ayırabilecek bir hiper düzlem bulmayı amaçlar. Fine Gaussian SVM, Gaussian çekirdek fonksiyonu kullanarak doğrusal olmayan ayrımları da dikkate alır ve bu sayede karmaşık sınıflandırma problemlerinde yüksek doğruluk oranları elde edebilir.

Gerçekleştirilen karşılaştırmalar sonucunda, bu iki modelin diğer yöntemlere kıyasla daha üstün performans sergilediği tespit edilmiştir. Bu nedenle, çalışmanın devamında bu modeller üzerine yoğunlaşarak, radar tabanlı insan sınıflandırma sistemlerinde kullanılmak üzere optimize edilmiş sınıflandırıcılar geliştirilmesi planlanmaktadır.

Fine Gaussian SVM modelinin matematiksel temeli, veri noktalarını yüksek boyutlu bir özellik uzayına eşleyen bir çekirdek fonksiyonu kullanmasına dayanır. Gaussian SVM'in karar fonksiyonu şu şekilde ifade edilebilir:

$$f(x) = \text{sign}\left(\sum_{i=1}^{n} \alpha_i y_i K(x_i, x) + b\right) \tag{3.3}$$

Burada:

- x: Sınıflandırılacak yeni veri noktası
- x_i: Eğitim veri setindeki i. destek vektörü
- y_i: x_i'nin sınıf etiketi (+1 veya -1)
- α_i: Lagrange çarpanı
- $K(x_i, x)$: Çekirdek fonksiyonu
- b: Bias terimi

Gaussian SVM'de kullanılan radyal tabanlı çekirdek fonksiyonu (RBF) şu şekildedir:

$$K(x_i, x) = \exp\left(-\frac{\|x_i - x\|^2}{2\sigma^2}\right) \tag{3.4}$$

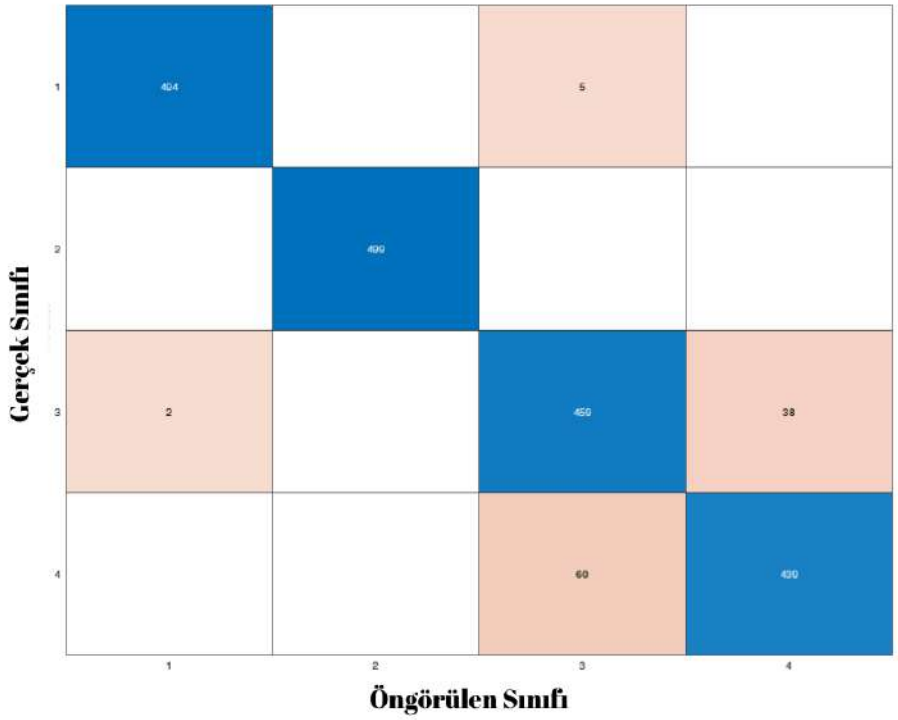
Burada σ parametresi, çekirdek fonksiyonunun genişliğini kontrol eder ve modelin "ince" ayarını belirler. Küçük σ değerleri, modelin daha karmaşık ve esnek olmasını sağlar, bu da "Fine" Gaussian SVM'in karakteristik özelliğidir.

3.2.1. Klasik Analiz Yönteminin Başarımının Ölçülmesi

Klasik analiz yöntemleri kullanılarak elde edilen sınıflandırıcı, MatlabCoder yardımıyla embedded sistemler için uygun bir şekilde C diline port edilmiştir. Bu işlem sonucunda, veri toplama cihazı içerisine entegre edilen sınıflandırıcı, saha testleri için üç gün süreyle sahada bırakılmıştır. Bu süre zarfında toplanan

verilerin analizi, insan ve hayvan sınıflandırmasında oldukça yüksek bir doğruluk oranı elde edildiğini göstermiştir.

Şekil 3.5, klasik analiz yöntemleri ile gerçekleştirilen sınıflandırmanın sonuçlarını göstermektedir. Şekildeki karmaşıklık matrisi, çeşitli sınıflar için doğru ve yanlış sınıflandırma sonuçlarını detaylı bir şekilde sunmaktadır. Özellikle, insan ve hayvan sınıflandırmasında elde edilen yüksek doğruluk oranları, klasik analiz yöntemlerinin bu tür sistemler için etkin bir çözüm sunduğunu kanıtlamaktadır.



Şekil 3.5: Klasik analiz yöntemi ile elde edilen sınıflandırma sonuçlarının karmaşıklık matrisi.

Sonuçlar, klasik analiz yöntemleri kullanılarak gerçekleştirilen bu yaklaşımın, sahada uygulanabilirliği ve sınıflandırma doğruluğu açısından güvenilir bir yöntem olduğunu göstermektedir. Önerilen yöntemin genel başarı oranı %94,74 olarak elde edilmiştir. Bu yüksek başarı oranı, sistemin farklı senaryolarda etkin bir şekilde çalışabildiğini ve hedef sınıflandırmasında doğru sonuçlar üretebildiğini göstermektedir.

Sınıflandırma işleminde kullanılan veri sınıfları ve her bir sınıf için elde edilen başarım seviyeleri aşağıda detaylandırılmıştır:

1. **Radarın Önünün Boş Olduğu Durum:**

   Bu senaryoda, radar algılama alanında herhangi bir hedef nesne bulunmamaktadır. Sistem, bu durumu doğru bir şekilde tespit ederek %98,79 başarı oranına ulaşmıştır. Bu yüksek oran, sistemin yanlış pozitif tespitleri minimumda tutarak güvenilir bir şekilde çalıştığını göstermektedir.

2. **Hedef Nesnenin Radara Çok Yakın Olduğu Durum:**

   Hedef nesnenin radara çok yakın mesafede bulunduğu ve sinyal yansımasının yoğun olduğu bu senaryoda, sistem %100 başarı oranı elde etmiştir. Bu sonuç, sistemin yakın mesafedeki hedefleri doğru bir şekilde algılama ve sınıflandırma kabiliyetinin mükemmel olduğunu göstermektedir.

3. **Hedef Nesnenin Bir Hayvan Olduğu Durum:**

   Radar tarafından algılanan hedefin bir hayvan olduğu durumlarda, sistem %91,98 başarı oranı ile doğru sınıflandırma yapmıştır. Bu yüksek oran, sistemin hayvan ve insan hedeflerini ayırt etmede etkili olduğunu ve hayvan hareketlerinin karakteristik özelliklerini başarılı bir şekilde tanıyabildiğini göstermektedir.

4. **Hedef Nesnenin Bir İnsan Olduğu Durum:**

   Hedef nesnenin bir insan olduğu senaryolarda, sistem %87,97 başarı oranı ile doğru sınıflandırma gerçekleştirmiştir. Bu sonuç, insan hareketlerinin doğru bir şekilde tespit edildiğini ve sistemin güvenilir bir insan sınıflandırma performansına sahip olduğunu göstermektedir.

Yukarıda sunulan sonuçlar, sistemin genel olarak yüksek bir doğrulukla çalıştığını ve farklı senaryolarda hedefleri başarılı bir şekilde sınıflandırabildiğini göstermektedir. Özellikle radarın önünün boş olduğu

ve hedef nesnenin radara çok yakın olduğu durumlarda elde edilen yüksek başarı oranları, sistemin temel algılama yeteneklerinin güçlü olduğunu ortaya koymaktadır.

Bununla birlikte, insan hedeflerinin sınıflandırılmasında elde edilen %87,97'lik başarı oranı, geliştirilme potansiyeline işaret etmektedir.

Sonuç olarak, bu çalışma klasik analiz yöntemleri kullanılarak geliştirilen yaklaşımın, sahada uygulanabilirliği ve sınıflandırma doğruluğu açısından güvenilir bir yöntem olduğunu göstermiştir. Elde edilen yüksek başarı oranları, sistemin farklı hedefleri etkin bir şekilde sınıflandırabildiğini ortaya koymaktadır. Gelecekteki çalışmalar, önerilen iyileştirmeler ve daha ileri tekniklerin entegrasyonu ile sistem performansını daha da artırabilir ve radar tabanlı sınıflandırma sistemlerinin gelişimine katkı sağlayabilir.

3.3. YENİ SALDIRI YÖNTEMİNİN GELİŞTİRİLMESİ

3.3.1. Radar Karıştırıcı Tipleri

Radar karıştırıcı, radar sinyallerine müdahale etmek için tasarlanmış elektronik cihazların genel adıdır. Bu cihazların genel hedefi kurban cihazların çalışmasını etkilemek, onların veri toplama süreçlerini etkilemek veya tamamen durdurmaktır. Radar Karıştırıcılar genellikle radar tabanlı sistemlerden kaçmak veya onları yanıltmak amacıyla kullanılırlar. Farklı radar türlerine ve özelliklerine göre çalışan çeşitli tiplerde radar karıştırıcılar mevcuttur. Ana radar karıştırıcı tipleri şu şekilde sıralanabilir

Gürültü Karıştırıcılar: Geniş bantlı gürültü üreterek radarın frekans bandını maskeler, böylece radarın geri dönen sinyali algılamasını engeller. Bu tür karıştırıcılar eğer belirli bir radar frekansında şalışıyorlarsa bu karıştırıcılara spot gürültü karıştırıcılar denir. Birden fazla frekansı kapsamak için geniş bir frekans çalışıyorlarsa bu tür karıştırıcılara Barrage gürültü karıştırıcılar denir. Bir çok karıştırıcı bandı arasında atlamalar yaparak çalışıyorlarsa bu tür karıştırıcılara Swept-Spot gürültü karıştırıcılar denir.

Gürültü karıştırıcıları aşağıdaki formül ile ifade edilebilir:

$$S_J(t) = \sqrt{2P_J} \cdot n(t) \cdot \cos(2\pi f_c t + \phi(t)) \tag{3.5}$$

Burada:

- $S_J(t)$: Karıştırıcı sinyali
- P_J: Karıştırıcının ortalama gücü
- $n(t)$: Birim güçlü beyaz Gauss gürültüsü
- f_c: Taşıyıcı frekans
- $\phi(t)$: Rastgele faz terimi

Bu formül, gürültü karıştırıcının temel çalışma prensibini göstermektedir. Karıştırıcı, radarın çalışma frekansında (f_c) yüksek güçlü (P_J) bir gürültü sinyali üreterek, radarın hedef tespitini zorlaştırır veya imkansız hale getirir.

Aldatıcı Karıştırıcılar: Hedef hakkında yanlış veya yanıltıcı bilgi yaratmak için radar sinyalini manipüle eder. Menzil kapısı kaydırma karıştırıcıları hedeflerin menzil değerlerini değiştirerek onların radar tarafından algılanmasını zorlaştırır. Hız kapısı kaydırma karıştırıcıları ise hedefin algılanan hızını değiştirerek onun radar tarafından algılanmasını zorlaştırır. Yineleyici karıştırıcılar radar sinyalini yakalayıp gecikmeli veya değiştirilmiş bir şekilde yeniden ileterek, radarın hedefin konumu veya hareketi hakkında yanılmasını sağlar.

Menzil Karıştırıcıları: Menzil karıştırıcıları, radarın hedef mesafesini yanlış algılamasına neden olur. Bu tür karıştırıcılar, radar sinyalini alır, geciktirir ve tekrar yayınlar. Menzil karıştırıcının ürettiği sinyal şu şekilde ifade edilebilir:

$$S_R(t) = A \cdot s(t - \tau) \cdot \cos(2\pi f_c t + \phi) \tag{3.6}$$

Burada:

- $S_R(t)$: Karıştırıcı sinyali
- A: Sinyal genliği
- $s(t)$: Orijinal radar sinyali
- τ: Gecikme süresi
- f_c: Taşıyıcı frekans
- ϕ: Faz kayması

Hız Karıştırıcıları: Hız karıştırıcıları, radarın hedef hızını yanlış algılamasına neden olur. Bu karıştırıcılar, radar sinyalinin frekansını değiştirerek çalışır. Hız karıştırıcının ürettiği sinyal şu şekilde ifade edilebilir:

$$S_V(t) = A \cdot s(t) \cdot \cos(2\pi(f_c + f_d)t + \phi) \tag{3.7}$$

Burada:

- $S_V(t)$: Karıştırıcı sinyali
- A: Sinyal genliği
- $s(t)$: Orijinal radar sinyali
- f_c: Taşıyıcı frekans
- f_d: Doppler frekans kayması
- ϕ: Faz kayması

Menzil karıştırıcıları ve hız karıştırıcıları arasındaki temel fark, manipüle ettikleri sinyal özelliğidir. Menzil karıştırıcıları, sinyalin zamanlamasını değiştirerek hedefin mesafesini yanıltırken, hız karıştırıcıları sinyalin

frekansını değiştirerek hedefin hızını yanıltır. Menzil karıştırıcıları τ gecikme parametresi ile çalışırken, hız karıştırıcıları f_d doppler frekans kayması parametresi ile çalışır. Bu farklı yaklaşımlar, radarın farklı ölçüm parametrelerini (mesafe veya hız) etkileyerek yanıltıcı sonuçlar elde etmesine neden olur.

Darbe Karıştırıcılar: Radar sinyaliyle senkronize olarak darbeler yayar, bu da radarın birden fazla yankı almasına ve hedefi doğru şekilde belirlemesinin zorlaşmasına neden olur. Bu karıştırıcılar, radar sinyalini algılar ve hemen ardından bir dizi sahte yankı üretir. Bu sahte yankılar, gerçek hedefin etrafında bir "yankı bulutu" oluşturarak, radarın hedefi doğru bir şekilde izlemesini engeller. Darbe karıştırıcılar, özellikle hedef takip radarlarına karşı etkilidir ve genellikle elektronik karşı tedbir (ECM) sistemlerinin önemli bir bileşenidir. Bu karıştırıcılar, radar operatörünün ekranında birden fazla sahte hedef görüntüsü oluşturarak, gerçek hedefin hangi sinyal olduğunu belirlemesini zorlaştırır. Ayrıca, bu karıştırıcılar radar sisteminin otomatik hedef takip algoritmalarını da yanıltabilir, böylece radar sistemi yanlış hedefleri takip etmeye başlayabilir.

Darbe karıştırıcıların ürettiği sinyal matematiksel olarak şu şekilde ifade edilebilir:

$$S_P(t) = \sum_{k=0}^{N-1} A_k \cdot p(t - kT) \cdot \cos(2\pi f_c t + \phi_k) \tag{3.8}$$

Burada:

- $S_P(t)$: Darbe karıştırıcı sinyali
- N: Toplam darbe sayısı
- A_k: k. Darbe genliği
- $p(t)$: Darbe şekli fonksiyonu
- T: Darbeler arası süre

- f_c: Taşıyıcı frekans
- ϕ_k: k. Darbe faz kayması

Bu formül, darbe karıştırıcının bir dizi senkronize darbe üreterek radar sinyalini nasıl manipüle ettiğini göstermektedir. Her bir darbe, belirli bir genlik, zamanlama ve faz ile üretilir, bu da radarın birden fazla sahte hedef algılamasına neden olur.

Çapraz-Göz Karıştırıcılar: Radar sinyalinin fazı değiştirilmiş versiyonlarını ileterek, radarın hedefin yönü hakkında yanlış bilgi almasına neden olur.

Çapraz-göz karıştırıcıların ürettiği sinyal matematiksel olarak şu şekilde ifade edilebilir:

$$S_C(t) = A \cdot s(t) \cdot \cos(2\pi f_c t + \phi(t)) \tag{3.9}$$

Burada:

- $S_C(t)$: Çapraz-göz karıştırıcı sinyali
- A: Sinyal genliği
- $s(t)$: Orijinal radar sinyali
- f_c: Taşıyıcı frekans
- $\phi(t)$: Zamana bağlı faz modülasyonu

$\phi(t)$ fonksiyonu, radarın yön algılama mekanizmasını yanıltmak için özel olarak tasarlanmış bir faz modülasyonudur. Bu modülasyon, radarın açısal ölçümlerini bozarak hedefin konumu hakkında yanlış bilgi üretmesine neden olur.

Akıllı Karıştırıcılar: Belirli radar türlerini tespit etmek ve onları hassas bir şekilde karıştırmak için gelişmiş algoritmalar kullanır. Bu tür karıştırıcılar,

enerji kullanımını optimize eder ve algılama riskini azaltarak radar sinyalini analiz ettikten sonra hedefe yönelik bir yanıt verir.

Her bir karıştırıcı tipi, karşı konulacak radar sistemi ve operasyonel hedeflere (örneğin, kaçış veya aldatma) göre farklı uygulamalara sahiptir

3.3.2. Bizim Saldırı Yöntemimiz

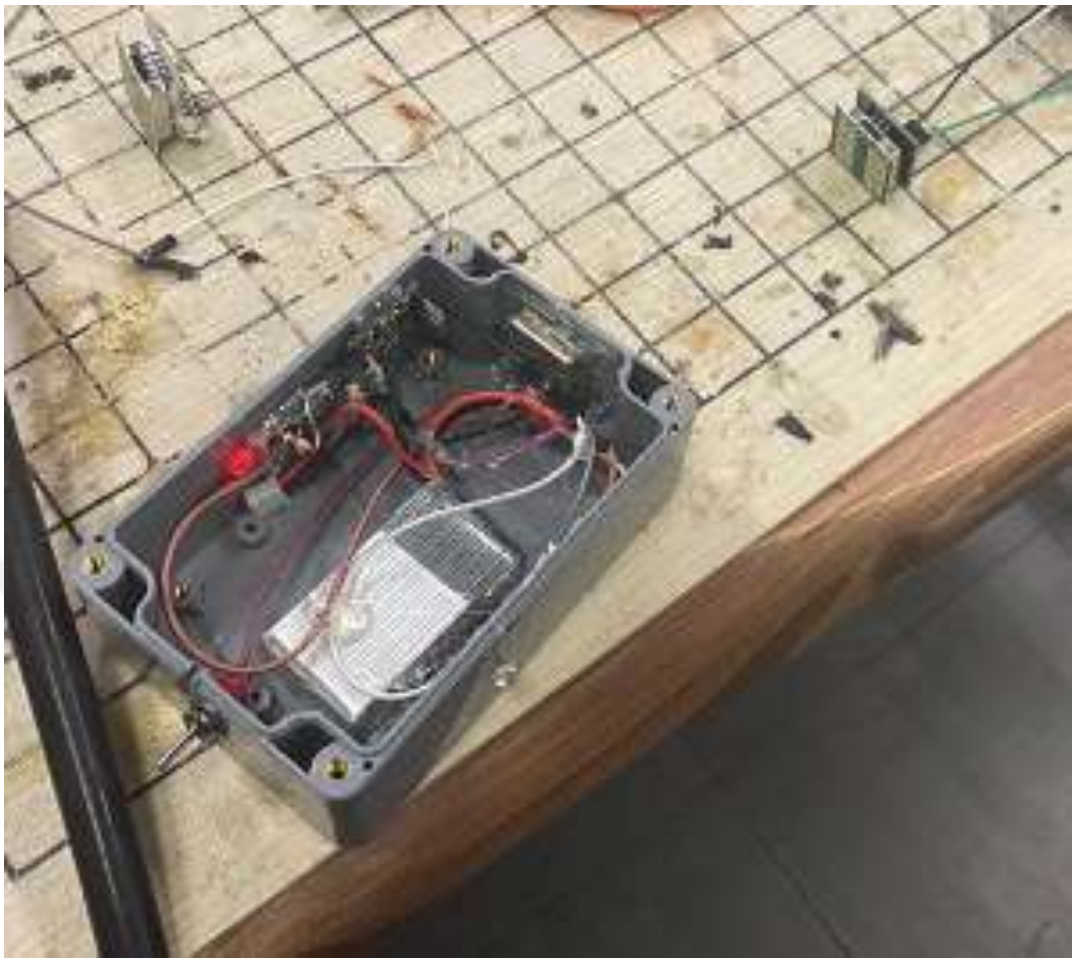
Mevcut elektronik donanımlar kullanılarak yeni bir saldırı yöntemi geliştirilmesi hedeflenmiştir. Bu amaç doğrultusunda, mevcut mikro doppler radarlar temel alınarak bir jammer cihazı tasarlanmıştır. Bu radarların temel çalışma prensibi, 24 GHz frekansında radyo sinyali yayını yapmaktır. Yayınlanan sinyalin hedeften geri dönüşünde meydana gelen değişiklikler, radar tarafından algılanarak bir sinyal üretilir. Bu bakımdan bir darbe karıştırıcı tasarlanmıştır. Darbe karıştırıcının çalışma prensipleri Fomül:3.10 ile ifade edilmektedir.

Hedef cihazın doğru veri almasını engellemek ve onu bloklamak amacıyla, hedef cihazın önüne yerleştirilen başka bir saldırgan cihaz kullanılmaktadır. Bu saldırgan cihaz, belirli aralıklarla açılıp kapanarak bir jamming etkisi oluşturur. Jamming etkisi, hedef cihazın algılama kabiliyetini zayıflatmakta ve doğru sınıflandırma yapmasını engellemektedir.

Kullanılan cihaz, yayın gücü bakımından zayıf olan (30 mV) bir mikro doppler radara dayanmaktadır. Bu durum, jamming etkisinin etkili olduğu mesafenin sınırlı olmasına yol açmıştır. Gerçekleştirilen testler sonucunda, bu menzilin 1 metreden daha kısa olduğu tespit edilmiştir. Dolayısıyla, cihazın etkili bir şekilde jamming yapabilmesi için hedefe çok yakın bir konumda bulunması gerekmektedir.

Bu saldırı yöntemi, radar tabanlı sistemlerin güvenlik açıklarını ortaya koymak amacıyla geliştirilmiştir. Bununla birlikte, jamming etkisinin daha uzak mesafelerde de etkin olabilmesi için gelecekteki çalışmalarda cihazın güçlendirilmesi ve optimizasyonu üzerine çalışmalar planlanmaktadır.

Elde mevcut bulunan elektronik donanımlarla yen bir saldırı yöntemi olması



Şekil 3.6: Jammer cihazı

için var olan mikro doppler radarlar kullanılmıştır. Bu radarları temel çalışma prensibi 24Ghz de radyo sinyal yayın yapmaktadır. Yapılan yayının geri dönüşünde oluşan değişime göre sinyal üretmektedir.

Bu durumda hedef cihazı bloklamak ve doğru veri almasını engellemek için hedef cihazın önüne bir başka saldırgan cihaz konularak bu cihazın açılıp kapanması sağlanarak jamming etkisi oluşturulmuştur.

Bu cihaz yayın gücü bakımından zayıf olan (10mV) bir mikro doppler radara dayanmaktadır. Bu nedenle jamming etkisinin etkili olduğu mesafe kısıtlı kalmıştır. Bu sebeple jamming verisi doğrudan veri toplama cihazı aracılığıyla toplanmıştır. Sonrasında bu verilere dayanarak önceden toplanan verilerin çeşitli jamming etkileri altında oluşacak sinyaller simule edilmiştir. Bu jamming seviyeleri, sırasıyla şöyledir;

Bu jamming etkisini matematiksel olarak şu şekilde ifade edebiliriz:

$$S_J(t) = S_N(t) + \alpha \cdot J(t) \tag{3.10}$$

Burada:

- $S_J(t)$: Karıştırılmış (jammed) sinyal
- $S_N(t)$: Normal radar sinyali
- $J(t)$: Karıştırıcı (jammer) sinyali
- α: Karıştırıcı sinyalinin ölçekleme faktörü

Ölçekleme faktörü α, istenen jamming gücü seviyesine bağlı olarak hesaplanır:

$$\alpha = \sqrt{\frac{P_J}{\overline{J^2(t)}}} \cdot \frac{2^{15}}{3} \tag{3.11}$$

Burada:

- P_J: İstenen jamming gücü (Watt cinsinden)
- $\overline{J^2(t)}$: Karıştırıcı sinyalinin ortalama kare değeri
- $2^{15}/3$: 16-bit tamsayı aralığını normalize etmek için kullanılan ölçekleme faktörü

Jamming gücü, dBm cinsinden verilen değerden Watt'a dönüştürülür:

$$P_J = 10^{(P_{dBm}-30)/10} \tag{3.12}$$

Son olarak, karıştırıcı sinyalinin sıfır ortalamalı olmasını sağlamak için bir düzeltme uygulanır:

$$J'(t) = J(t) - \overline{J(t)} \tag{3.13}$$

Bu matematiksel ifadeler, verilen kod parçasının işlevini açıklamaktadır. Karıştırıcı sinyali, istenen güç seviyesine göre ölçeklendirilerek normal radar sinyaline eklenir, böylece jamming etkisi oluşturulur.

1. 5 dB, 3.2mW, SNR 2.3272
2. 10 dB, 10mW, SNR 2.0913
3. 15 dB, 32mW, SNR 1.8554
4. 20 dB, 100mW, SNR 1.6195
5. 25 dB, 320mW, SNR 1.3835
6. 30 dB, 1.0W, SNR 1.1476
7. 40 dB, 10.0W, SNR 0.6758
8. 50 dB, 100.0W, SNR 0.2040

Bu sayede çok düşük karıştırma seviyesinden çok yüksek karıştırma seviyesine kadar olası tüm aralıkta karıştırma saldırısının ektisi ölçülerek buna uygun şekilde yapay zekanın geliştirilmesi sağlanacaktır.

3.3.3. Saldırı Yönteminin Başarımının Ölçülmesi

Saldırı yönteminin başarımını ölçmek için jammer cihazının önüne bir kayıt cihazı konularak kayıt örnekleri toplanmıştır.

Bu toparlanan veriler önceden toplanmış olan verilerle ortalama yöntemi ile karıştırılmıştır. **Şekil 3.9**, **Şekil 3.10** ve **Şekil 3.11** ham bir insan verisi örneği,

Şekil 3.7: Osiloskopta jammer sinyali

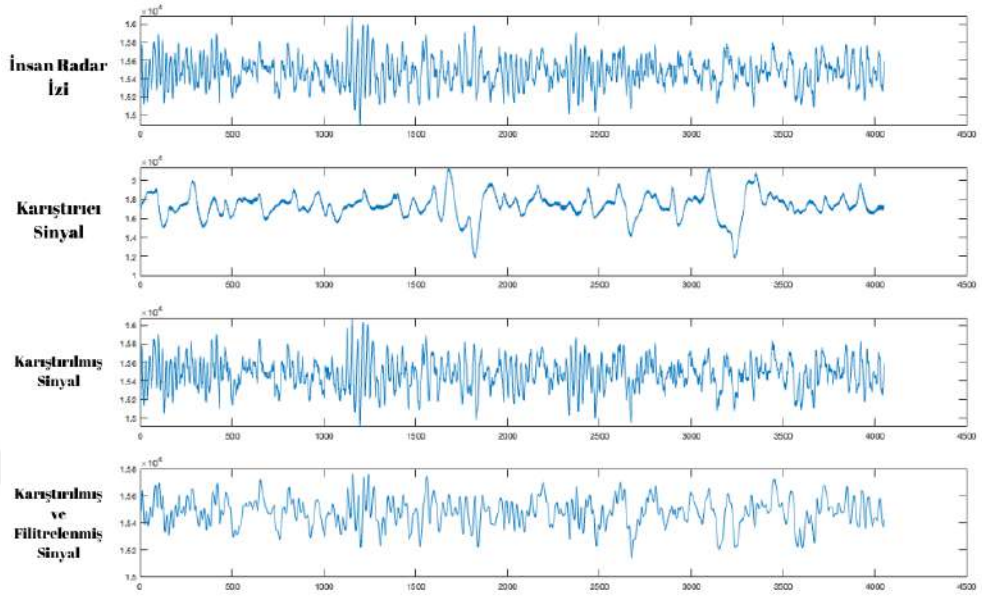
ham bir jammer verisi örneği, bir karıştırılmış veri örneği, ve bir filtrelenmiş veri örneği görebilirsiniz.

Bu durumdaki veri yapay zekâ temelli karar alma mekanizmasına sürülerek normal durumdaki hali ile karşılaştırılarak jamming mekanizmasının doğruluğu ölçülmüştür.

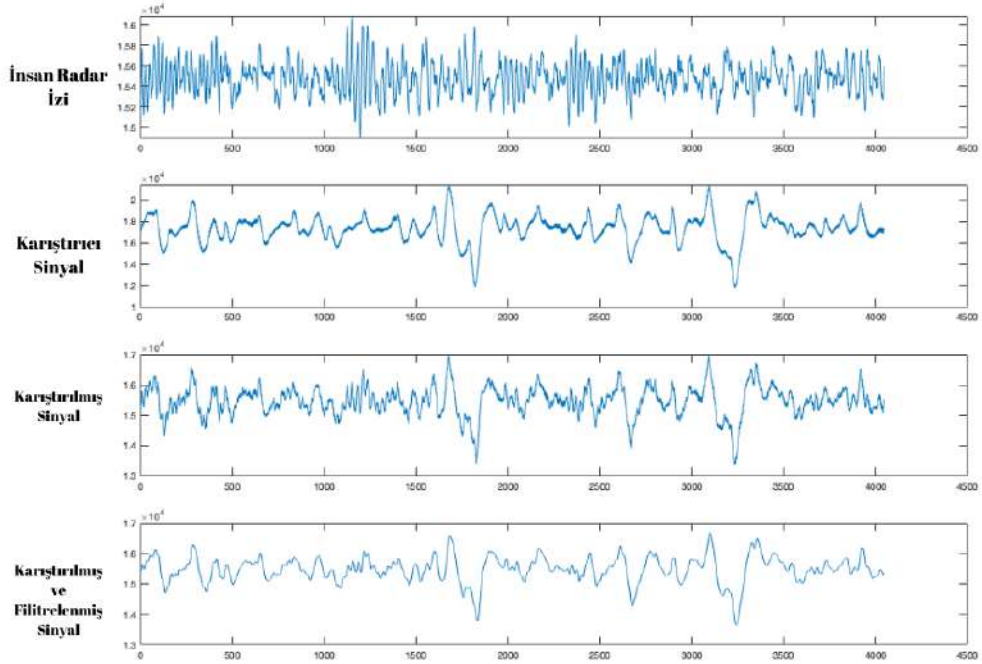
Burada ise ilgili radarın saldırı altında olması durumundaki başarım oranları verilmektedir.

1. Boş olma durumunda başarım %91,2 oranında düşmüştür. Burada ilgili yapay zeka, veri üzerinde bir hareket olduğunu anlayabilmiştir. Fakat bu, önceden saldırganlar hakkında eğitilmemiş olduğu için hareketin kaynağının saldırgan bir hedef olduğunu anlayamamıştır. Bu nedenle ilgili verileri 3. sınıf yani (insan olmayan herhangi bir hedef) olarak tanımlamıştır.
2. Hedefin aşırı yakın olma durumunda %6,3 oranında bir başarım düşüşü

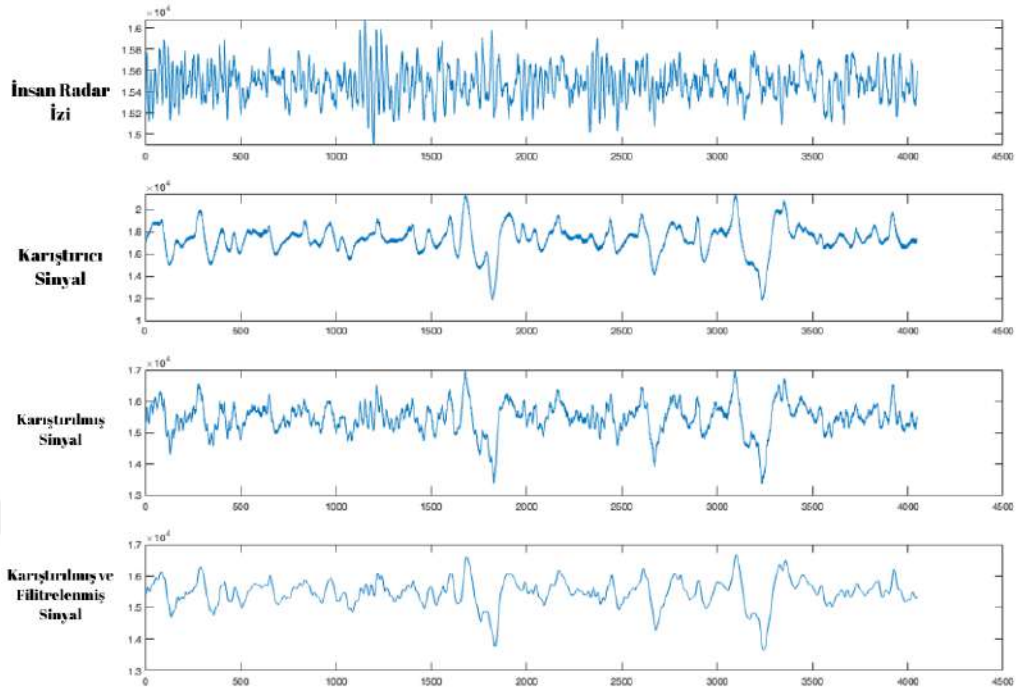
Şekil 3.8: Jammer ve veri toplama cihazı



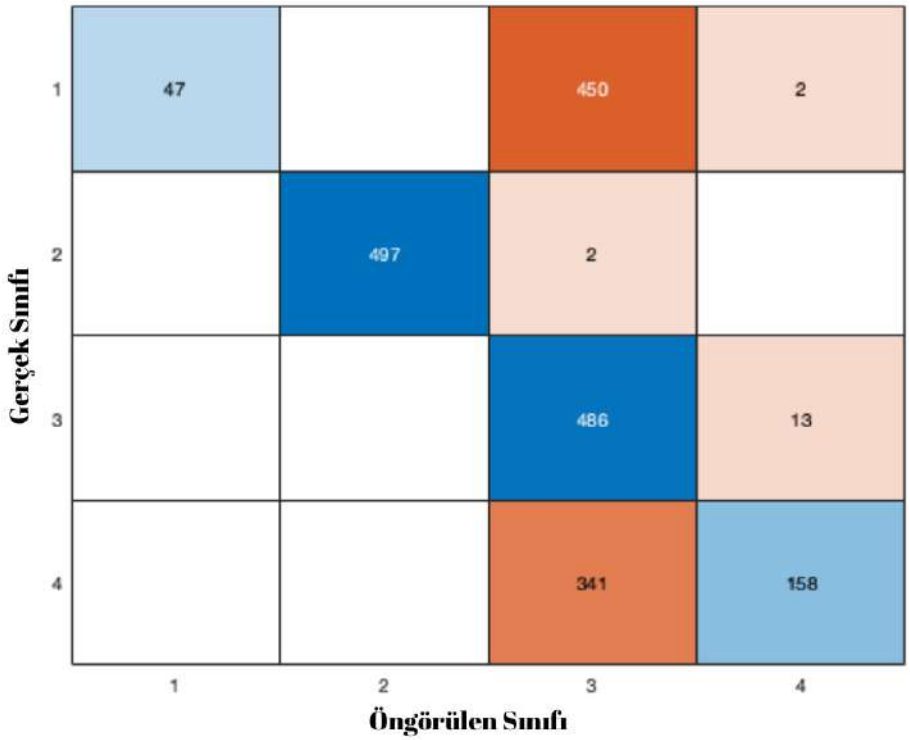
Şekil 3.9: 5 dB'de Radar ve karıştırıcı verileri



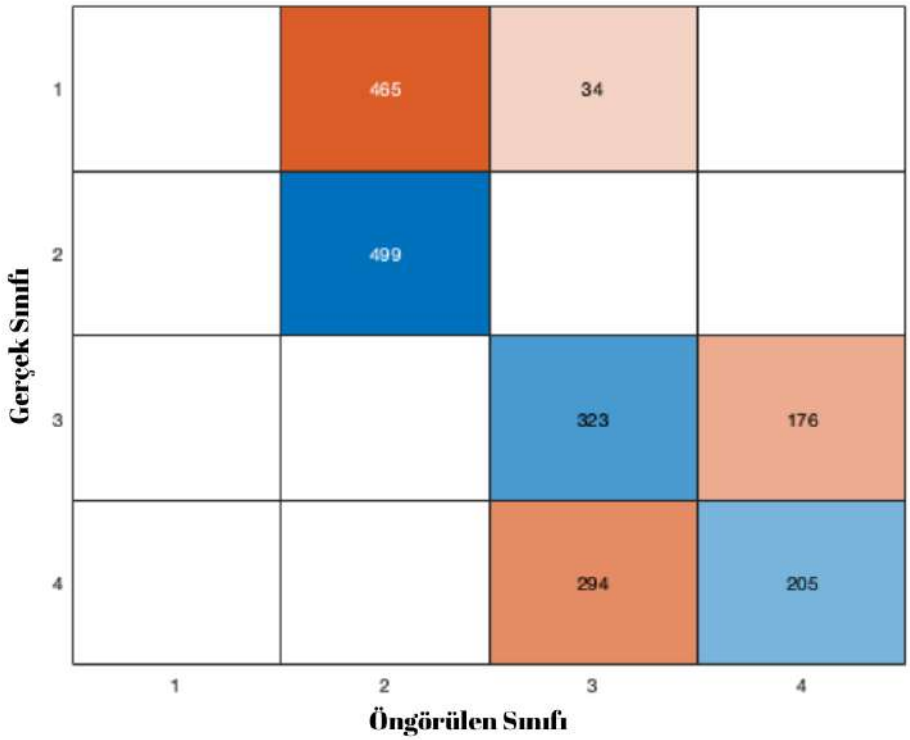
Şekil 3.10: 25 dB'de Radar ve karıştırıcı verileri



Şekil 3.11: 50 dB'de Radar ve karıştırıcı verileri



Şekil 3.12: 25 dB'de Jammer sınıflandırma bozulması



Şekil 3.13: 50 dB'de gürültü altında veri bozulması

yaşanmıştır.

3. Hedefin insan olmayan herhangi bir hayvan olması durumunu temsil eden 3. sınıfta başarım oranı yükselmiştir. Bunun sebebi, eğitilen yapay zekanın aslında insan varlığına özel olarak odaklanmasıdır. Bu bakımdan, yüksek çeşitliliğe sahip olan 3. sınıf, aslında insan olmayan herhangi bir hedef olarak eğitilmiştir. İlgili sınıfta, hayvanın cihaza yakın olması, fazla hareket etmemesi gibi durumlarda toplanan veriler boş olarak sınıflandırılmaktaydı. Bu durumda, ilgili veriler hareketliliğin kaynağı anlaşılamadığı için bu şekilde sınıflandırılmıştır.

4. İnsan hareketliliğine odaklanmış, yüksek doğrulukta bir sınıf olduğu için bu sınıfta %69,1'lik bir düşüş sağlanmıştır. Orijinal verilerde başarım oranının %72,2 olduğu göz önüne alınırsa, sistemin tamamen felç edildiği söylenebilir.

3.4. SALDIRI YÖNTEMİNE KARŞI ÖNLEM GELİŞTİRİLMESİ

Boche ve diğ. [73] yaptıkları çalışmada, bir iletişim kanalında karıştırma (jamming) yapılıp yapılmadığının bilinmesinin durdurma problemine (halting problem) eşdeğer bir problem olduğunu göstermişlerdir. Bu nedenle, iletişim kanalları açısından karıştırma saldırılarının kesin bir şekilde tespit edilmesi imkânsızdır.

Bu çalışmada, söz konusu zorluğun üstesinden gelmek ve karıştırma saldırılarına karşı dirençli bir sistem geliştirmek amacıyla, dört sınıflı karmaşık bir yapay zekâ modeli tasarlanmıştır: Bu geliştirilen yapayzeka modeli temelde önceki sınıflandırıcı ile aynı mekanizmaya sahiptir. Fakat bu modelde eğitilen veri seti karıştırmaya uğratılmış verilerle birlikte eğitilerek daha dirençli hale getirilmiştir. Bu bakımdan veri zenginleştirmesi aşamasının önemini vurgulamak gerekir.

Veri zenginleştirilmesi şu şekilde yapılmıştır. Veriseti önceki çalışmada olduğu gibi 4 sınıfa ayrılmış ve bu sınıflara ait verilere 5, 10, 15, 20, 25, 30, 40, 50 dB luk karıştırma seviyelerinde karıştıma yapılmıştır. Bu yapılan karıştımanın ardından veriler bölütlenmiştir ve her bir veri seti 4 farklı sınıfa ayrılmıştır. Bu sayede elde edilen yeni veri seti daha fazla sayıda veri içermekte ve her bir sınıfın da karıştırma altında farklı özellikleri yansıtmaktadır. Bu sayede yapay zeka modeli daha farklı ve karmaşık durumlarla uygun şekilde eğitilmektedir. Veri zenginleştirilmesi sistematiği ile ilgili sözde kodu aşşağıda verilmiştir.

```
Fonksiyon structToClassifierAddJammingData
    (data, maxCount, repeat, parts, partSize, jammerDatas)
    // Veri yapisinin alan adlarini al
    fnames = data'nin alan adlari
    kSize = fnames'in boyutu

    // Her bir veri sinifi icin islem yap
    Her i = 1'den kSize'a kadar paralel dongu:
        key = fnames[i]
        datas = data[key]
```

```
// Verileri karistir
datas'i rastgele sirala

// Jamming parametrelerini tanimla
jammingFactors = [0, 5, 10, 15, 20, 25, 30, 40, 50]

// Veri sayisini belirle
dataCount = datas'in satir sayisi
count = min(maxCount, dataCount) - 1

// Her bir veri icin islem yap
Her j = 1'den (count * repeat)'e kadar dongu:
    // Rastgele jamming faktoru ve veri sec
    jammingFactor = jammingFactors'dan rastgele sec
    jammerData = jammerDatas'dan rastgele sec
    currentData = datas'dan sirayla veri al

    // Jamming uygula ve Kalman filtresi ile filtrele
    jammedData = addJamming
        (currentData, jammerData, jammingFactor)

    filteredData = applyKalmanFilter(jammedData)

    // Bos veri kontrolu
    Eger i != 1 ve filteredData bos ise:
        Dongunun basina don

    // Veriyi parcalara ayir ve kaydet
    Her k = 1'den parts'a kadar dongu:
        subData = filteredData'dan partSize kadar al
        dat'a subData'yi ekle
```

```
// En kucuk veri boyutunu bul
varMnSize = en kucuk veri boyutunu hesapla

// Cikis verilerini olustur
outLab = kSize * varMnSize boyutunda sifir dizisi
outData = kSize * varMnSize x partSize boyutunda sifir matrisi

// Her sinif icin verileri duzenle
Her i = 1'den kSize'a kadar dongu:
    // Eksik verileri rastgele kopyalayarak tamamla
    Eksik verileri rastgele kopyalayarak tamamla

    // Cikis verilerini ve etiketlerini ata
    outData'nin ilgili kismina verileri yerlestir
    outLab'in ilgili kismina sinif etiketini ata

// Sonuclari dondur
Dondur outData, outLab, fnames
```

Veri seti entropisi, bir veri setindeki bilgi içeriğini ve belirsizliğini ölçen önemli bir kavramdır. Claude Shannon tarafından geliştirilen bu konsept, veri setinin karmaşıklığını ve içerdiği bilginin miktarını sayısal olarak ifade eder. Entropi, veri setindeki çeşitliliği ve öngörülemezliği yansıtır.

Veri seti entropisi şu şekilde hesaplanır:

$$H = -\sum_{i=1}^{n} p_i \log_2(p_i) \tag{3.14}$$

Burada:

- H: Entropi değeri
- n: Veri setindeki benzersiz sınıf veya kategori sayısı
- p_i: i. sınıfın görülme olasılığı

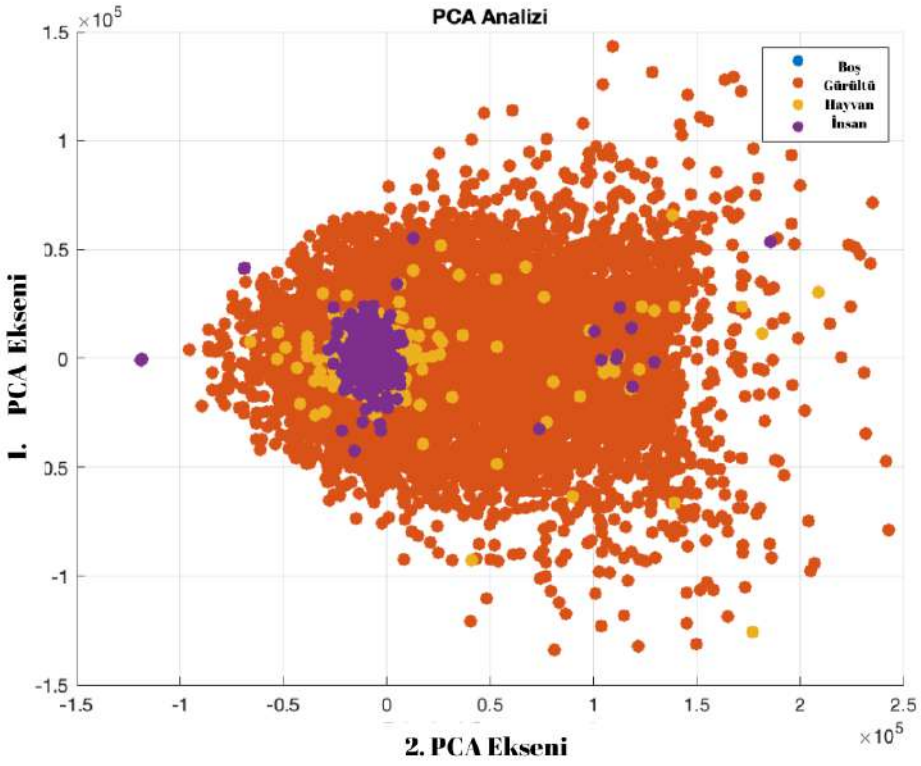
Veri seti entropisi, makine öğrenmesi ve yapay zeka alanlarında özellikle önemlidir:

1. **Model Performansı:** Yüksek entropiye sahip veri setleri genellikle daha zorlu öğrenme görevleri sunar ve modelin genelleme yeteneğini artırabilir.
2. **Veri Kalitesi:** Entropi, veri setinin bilgi içeriğini yansıttığından, veri kalitesinin bir göstergesi olarak kullanılabilir.
3. **Özellik Seçimi:** Yüksek entropiye sahip özellikler genellikle daha bilgilendiricidir ve model eğitiminde daha değerli olabilir.
4. **Aşırı Öğrenme Riski:** Düşük entropili veri setleri, modelin aşırı öğrenme (overfitting) riskini artırabilir.

Bu çalışmada, veri zenginleştirme süreci veri seti entropisini artırmıştır. Karıştırma saldırılarına ait verilerin eklenmesi, veri setindeki çeşitliliği ve karmaşıklığı artırarak daha yüksek bir entropi değerine yol açmıştır. Bu artış, modelin daha geniş bir senaryo yelpazesini öğrenmesine ve karıştırma saldırılarına karşı daha dirençli hale gelmesine katkıda bulunmuştur. Bu durum **Şekil 3.14** ve **Şekil 3.15** şekillerinde gösterilmektedir.

Bu şekillerin incelenidğinde görüleceği üzere boş olma durumunda veri seti entropisi. Şu şekilde ölçülmüştür öncelikle veri setinin PCA analizi yapılmaktadır sonrasında bu analiz sonucunda çıktının entropisi ölçülerek değerlendirilmektedir. Bunu nsebebi ise PCA analizi yapıldığında veri setinin daha az boyutlu hale getirilmesi sağlanmaktadır. Bu yöntemle ölçülen veriseti entropisi %58 oranında artmıştır. Bunun yanında boş olma durumu ve gürültü olma durumunada veri seti entropisinin benzer kaldığı hatta düştüğü görülmektedir. Burada yapılacak yorum şu şekildedir.

Boş Olma Durumu bu durum için veri seti entropisi sadece %3 oranda artmıştır ki buna aynı kalmıştır denilebilir. Bu durumun sabebi ölçüm yöntemimizle alakalı olarak değerlendirilmektedir. Çünkü önce veri setinin PCA analizi yapılmaktadır ki bu durum eldeki her iki veri setinin de kendi



Şekil 3.14: Karıştırma eklenmemiş veriseti dağıtık analizi.

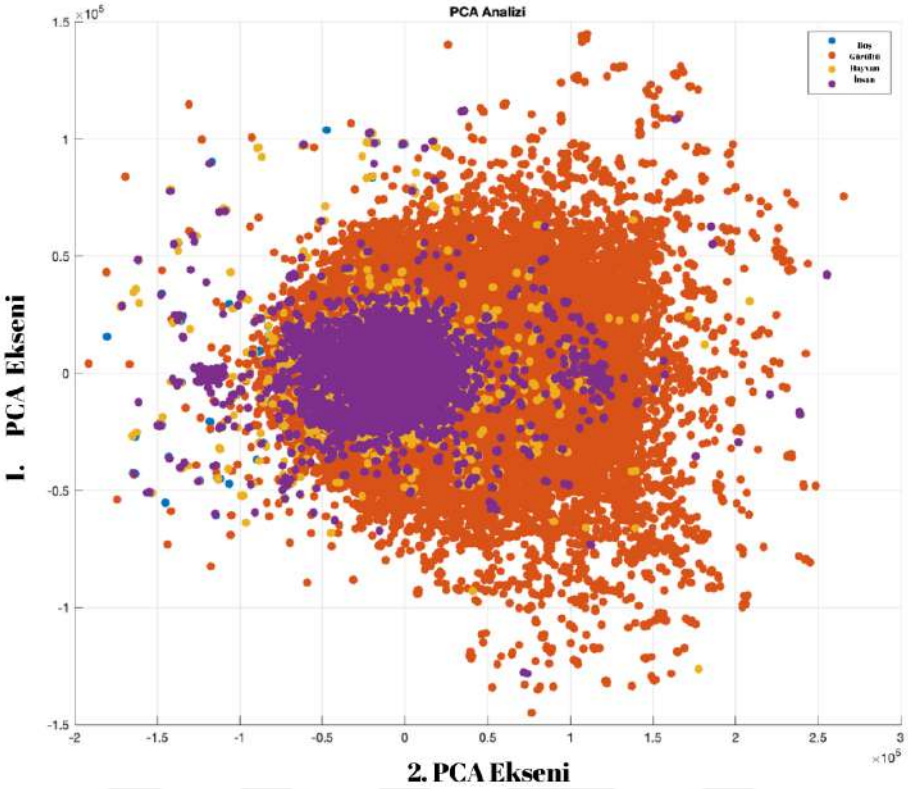
içindeki değerlere göre indirgenmesini getirmektedir. Sonuç olarak oluşan genel veri setinin entropisi artışı diğer sınıflara göre daha az olduğundan bu sınıfın içindeki entropi artışının görece az olması açıklanabilir.

Gürültü Olma Durumu Bu durumda ise veri seti entropisi %5 oranında azalmıştır. Bu durumda ise karıştırma yönteminin pulse gürültüler olarak yapılmasından kaynaklanmaktadır. Dolayısıla gerçek gürültülere kıyasla daha az karmaşık olan pulse gürültülerinin entropisi daha düşük çıkmaktadır.

Hayvan Hareketliliği Bu durumda ise veri seti entropisi %135 oranında artmıştır. En yüksek oranda artışın olduğu sınıf hayvan olma durumudur. Bu durumda ise hayvan hareketliliğinin yüksek olmasından kaynaklanmaktadır.

İnsan Hareketliliği Bu durumda ise veri seti entropisi %76 oranında artmıştır. Bu durumda ise insan hareketliliğinin yüksek olmasından kaynaklanmaktadır.

Bu modelin geliştirilmesinde, farklı düzeylerde karıştırma saldırılarına maruz kalmış veriler kullanılarak eğitim yapılmıştır. Bu şekilde eğitilen yapay zekâ



Şekil 3.15: Karıştırma eklenmiş veriseti dağıtık analizi.

modeli, olası karıştırma saldırılarına karşı çok daha dirençli hale getirilmiştir. Model, hem saldırı tespitinde hem de hedef sınıflandırmasında yüksek bir başarı oranı sergilemektedir, bu da radar tabanlı sistemlerin güvenilirliğini artırmaktadır.

3.4.1. Karşı Önlemin Başarımının Ölçülmesi

Yeni geliştirilen karıştırmaya duyarlı sınıflandırıcı kullanılarak kapsamlı testler gerçekleştirilmiştir. Bu testler, sistemin farklı senaryolarda karıştırma saldırılarına karşı performansını değerlendirmeyi amaçlamaktadır.

20 dB gürültü seviyesi için elde edilen sonuçlar **Şekil 3.16**'de gösterilmektedir. Aşağıda, farklı durumlar için başarım seviyeleri ayrıntılı olarak sunulmuştur:

1. **Boş Olma Durumu:**

   Karıştırma saldırısı altında, sistemin başarım seviyesi %98,99'dan %14,44'e düşmüştür. Ancak, önerilen karşı önlemin uygulanmasıyla

birlikte başarım seviyesi %95,19'a yükselmiştir.

2. **Çok Yakın Olma Durumu:**

   Başarım seviyesi, karıştırma etkisiyle %100'den %99,79'a düşmüştür. Karşı önlem ile bu değer %98,99 olarak iyileştirilmiştir.

3. **Hayvan Olma Durumu:**

   Sistemin başarımı, karıştırma altında %91,98'den %96,99'a yükselmiştir. Karşı önlem uygulandığında ise başarım seviyesi %86,57 olarak kaydedilmiştir.

4. **İnsan Olma Durumu:**

   Karıştırma saldırısı, başarım seviyesini %87,97'den %55,11'e düşürmüştür. Geliştirilen karşı önlem sayesinde bu değer %72,94'e yükselmiştir.

Elde edilen sonuçlar, önerilen karşı önlemin karıştırma saldırılarının olumsuz etkilerini önemli ölçüde azalttığını göstermektedir. Özellikle boş olma ve insan olma durumlarında gözlenen iyileştirmeler, sistemin güvenilirliğini artırmada karşı önlemin etkinliğini ortaya koymaktadır.

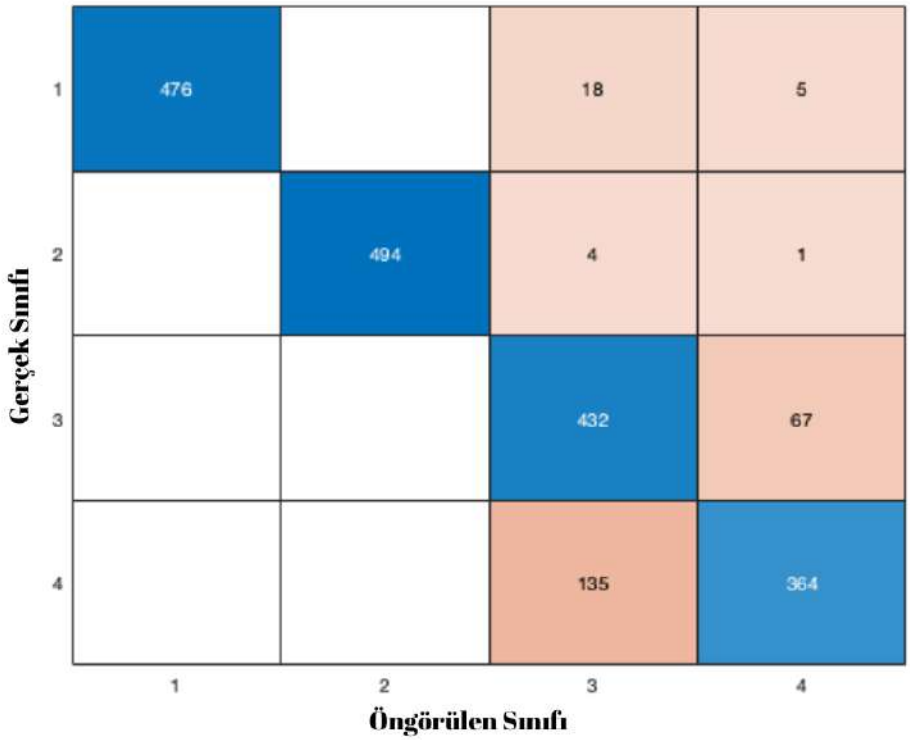
Benzer şekilde, 25 dB gürültü seviyesi için de testler gerçekleştirilmiş ve sonuçlar **Şekil 3.17**'de sunulmuştur. Elde edilen başarım seviyeleri aşağıda detaylandırılmıştır:

1. **Boş Olma Durumu:**

   Karıştırma saldırısı altında, sistemin başarım seviyesi %98,99'dan %9,41'e düşmüştür. Önerilen karşı önlemin uygulanmasıyla birlikte, başarım seviyesi %70,14'e yükseltilmiştir.

2. **Çok Yakın Olma Durumu:**

   Başarım seviyesi, karıştırma etkisiyle %100'den %99,05'e düşmüştür. Karşı önlem uygulandığında bu değer %99,39'a yükselmiştir.



Şekil 3.16: Karıştırıcı Önlemi Etkinliği 20dB de

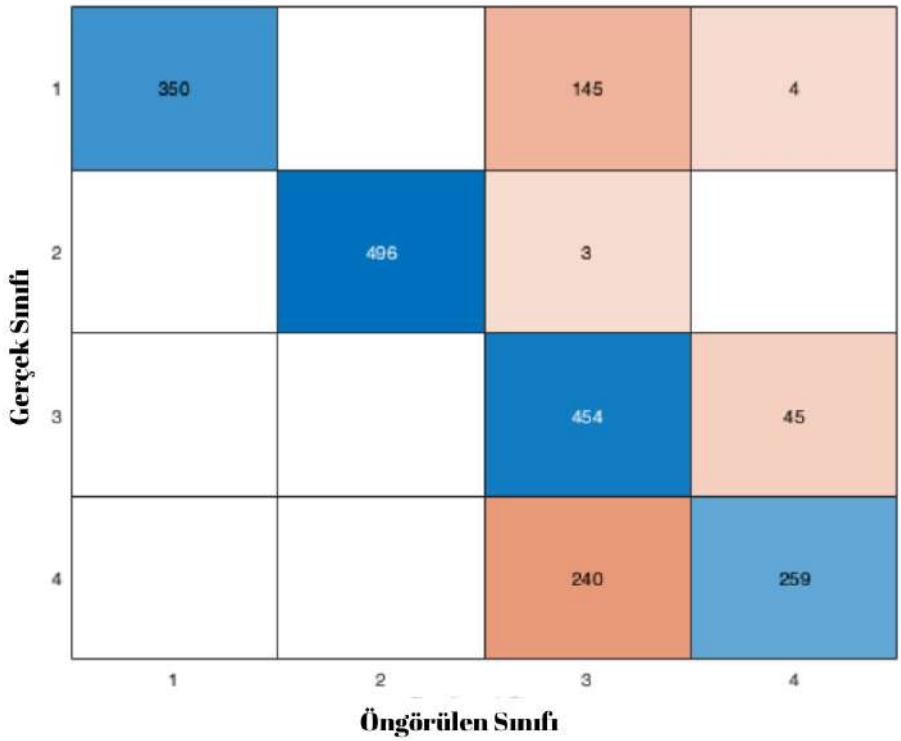
3. **Hayvan Olma Durumu:**

   Sistemin başarımı, karıştırma altında %91,98'den %97,39'a yükselmiştir. Karşı önlem uygulandığında ise başarım seviyesi %90,78 olarak kaydedilmiştir.

4. **İnsan Olma Durumu:**

   Karıştırma saldırısı, başarım seviyesini %87,97'den %31,66'ya düşürmüştür. Geliştirilen karşı önlem sayesinde bu değer %51,80'e yükseltilmiştir.

Bu sonuçlar, 25 dB gürültü seviyesinde de önerilen karşı önlemin etkinliğini ortaya koymaktadır. Özellikle boş olma ve insan olma durumlarında gözlenen iyileştirmeler, sistemin karıştırma saldırılarına karşı dirençliliğini artırmada karşı önlemin önemli bir rol oynadığını göstermektedir.



Şekil 3.17: Karıştırıcı Önlemi Etkinliği 25dB de

4. BULGULAR

Bu çalışma kapsamında, insan ve hayvan sınıflandırması yapan doppler radar sistemlerine yönelik sahtekarlık (spoofing) saldırılarının tespiti ve önlenmesi amacıyla kapsamlı bir araştırma yürütülmüştür. Bu amaçla, özgün bir Sürekli Dalga (Continuous Wave, CW) radar tabanlı veri toplama cihazı geliştirilmiş ve gerçek dünya koşullarını yansıtan geniş kapsamlı bir veri seti oluşturulmuştur. Oluşturulan bu veri seti, hem mevcut çalışmanın sağlamlığını artırmakta hem de gelecekteki araştırmalar için değerli bir kaynak potansiyeli taşımaktadır.

4.1. TOPLANAN VERİ SETİ

Veri setinin içeriği ve yapısı aşağıda detaylı olarak sunulmuştur:

1. **İnsan Yürüyüşü:**

   Toplam 228 saniye kayıt.

   İnsan yürüyüşü verileri, insan hareketinin en temel biçimlerinden birini temsil etmektedir. Bu veriler, sistemin insan hareketini doğru bir şekilde tanımlaması ve sahtekarlık girişimlerini tespit etmesi açısından kritik öneme sahiptir.

2. **İnsan Grup Yürüyüşü:**

   Toplam 321 saniye kayıt.

   Grup halinde yürüyen insanların verileri, radar sisteminin birden fazla hedefi ayırt edebilme yeteneğini test etmektedir. Bu, kalabalık ortamlarda veya birden fazla insanın bulunduğu senaryolarda sistemin etkinliğini değerlendirmek için değerlidir.

3. **İnsan Zıplama:**

   Toplam 25 saniye kayıt.

Zıplama hareketi, standart yürüme ve koşma hareketlerinden farklı bir hareket paternine sahiptir. Bu veriler, sistemin farklı insan hareketlerini ayırt etme kabiliyetini artırmaktadır.

4. **İnsan Metal Sopa ile Yürüme:**

   Toplam 48 saniye kayıt.

   Metal bir nesne ile yürüyen insan verileri, radar sinyallerinde farklı yansımalar oluşturarak sistemin metal nesneleri algılama ve sınıflandırma yeteneğini test etmektedir. Bu, güvenlik uygulamaları için önemli bir özelliktir.

5. **İnsan Koşma:**

   Toplam 131 saniye kayıt.

   Koşma hareketi, yürüme hareketinden farklı dinamiklere sahiptir. Bu veriler, sistemin farklı hızlardaki insan hareketlerini doğru bir şekilde sınıflandırmasını sağlamaktadır.

6. **Köpek Koşma:**

   Toplam 32 saniye kayıt.

   Köpeklerin koşma verileri, hayvan hareketlerinin dinamiklerini anlamak ve insan hareketleri ile karşılaştırmak için değerlidir. Bu, sistemin insan ve hayvan ayrımında daha hassas olmasını sağlar.

7. **At Dolaşma:**

   Toplam 523 saniye kayıt.

   Atların hareketleri, büyük hayvan hareketlerinin radar imzalarını anlamak için önemlidir. Bu veriler, sistemin farklı boyutlardaki hayvanları tanımlama kabiliyetini geliştirmektedir.

8. **Eşek Dolaşma:**

   Toplam 16 saniye kayıt.

   Eşek hareketleri, benzer boyutlardaki hayvanların ayrımını yapmak için kullanılmaktadır. Bu, sınıflandırma algoritmalarının hassasiyetini artırır.

9. **Geyik:**

   Toplam 541 saniye kayıt.

   Geyik verileri, vahşi hayvan hareketlerinin radar imzalarını elde etmek için önemlidir. Bu, özellikle ormanlık alanlardaki uygulamalar için değerlidir.

10. **Koyun:**

    Toplam 523 saniye kayıt.

    Koyun hareketleri, sürü davranışlarını ve küçük hayvan hareketlerini anlamak için toplanmıştır. Bu, sistemin farklı hayvan türlerini ayırt etme yeteneğini geliştirir.

11. **Cüce Domuz:**

    Toplam 230 saniye kayıt.

    Cüce domuz verileri, küçük ve orta boy hayvanların radar imzalarını elde etmek için önemlidir. Bu, sistemin çeşitli hayvan boyutlarını tanımasını sağlar.

12. **Kurt:**

    Toplam 241 saniye kayıt.

    Kurt hareketleri, yırtıcı hayvanların dinamiklerini anlamak için toplanmıştır. Bu, güvenlik ve vahşi yaşam izleme uygulamalarında kritiktir.

13. **Ceylan:**

    Toplam 107 saniye kayıt.

    Ceylan verileri, hızlı hareket eden hayvanların radar imzalarını elde etmek için değerlidir. Bu, sistemin yüksek hızlı hedefleri izleme kabiliyetini artırır.

14. **Keçi:**

    Toplam 255 saniye kayıt.

Keçi hareketleri, dağlık ve engebeli arazilerdeki hayvan hareketlerini anlamak için önemlidir. Bu veriler, sistemin çeşitli çevresel koşullarda performansını değerlendirmeye yardımcı olur.

15. **Boş (Arka Plan):**

    Toplam 825 saniye kayıt.

    Boş arka plan verileri, sistemin herhangi bir hedef olmadığında nasıl davrandığını anlamak için kritiktir. Bu, yanlış alarm oranlarının azaltılmasına katkı sağlar.

16. **Karıştırıcı (Jammer):**

    Toplam 202 saniye kayıt.

    Karıştırıcı verileri, sahtekarlık ve karıştırma saldırılarına karşı sistemin tepkisini değerlendirmek için önemlidir. Bu, güvenlik önlemlerinin geliştirilmesine yardımcı olur.

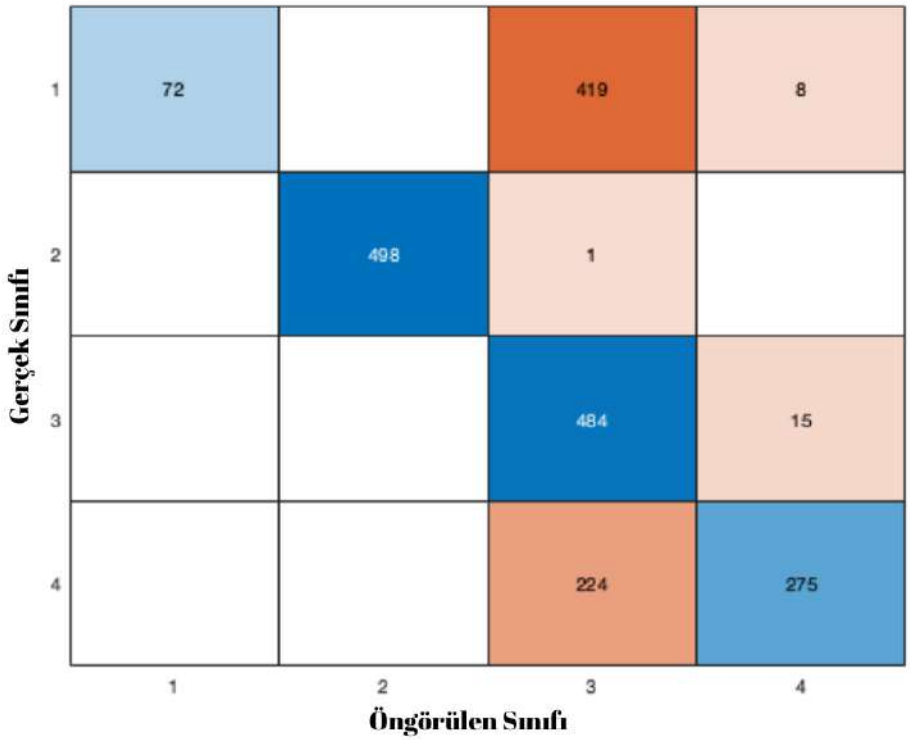
17. **Gürültü:**

    Toplam 199 saniye kayıt.

    Gürültü verileri, çevresel ve sistem kaynaklı gürültünün etkisini analiz etmek için kullanılmaktadır. Bu, sinyal işleme algoritmalarının iyileştirilmesine katkıda bulunur.

Bu kapsamlı veri seti, farklı insan ve hayvan hareketlerini içermekte ve sahtekarlık saldırılarına karşı sistemin performansını değerlendirmek için zengin bir kaynak sunmaktadır. Özellikle insan ve hayvan davranışlarının çeşitliliği, sınıflandırma algoritmalarının genel performansını ve güvenilirliğini artırmaya yönelik önemli bir katkı sağlamaktadır.

Toplanan kapsamlı veri seti kullanılarak, insan ve hayvanları etkin bir şekilde ayırt edebilen bir sınıflandırıcı başarıyla eğitilmiştir. Bu sınıflandırıcının performansı, çeşitli senaryolar altında test edilerek doğrulanmıştır. Ayrıca, orijinal bir sürekli dalga (CW) radar karıştırıcısı (*jammer*) geliştirilmiş ve bu cihaz aracılığıyla veri toplama sistemine yönelik aldatma (spoofing) saldırıları simüle edilmiştir. Bu saldırılar sonucunda elde edilen veriler, sınıflandırıcının



Şekil 4.1: 20 dB'de karıştırıcının sınıflandırma performansına etkisi

saldırı altındaki performansını değerlendirmek ve saldırılara karşı dirençli bir model geliştirmek için kullanılmıştır. Yapay zekânın bu koşullar altındaki etkinliği **Şekil 4.3**'de gösterilmektedir.

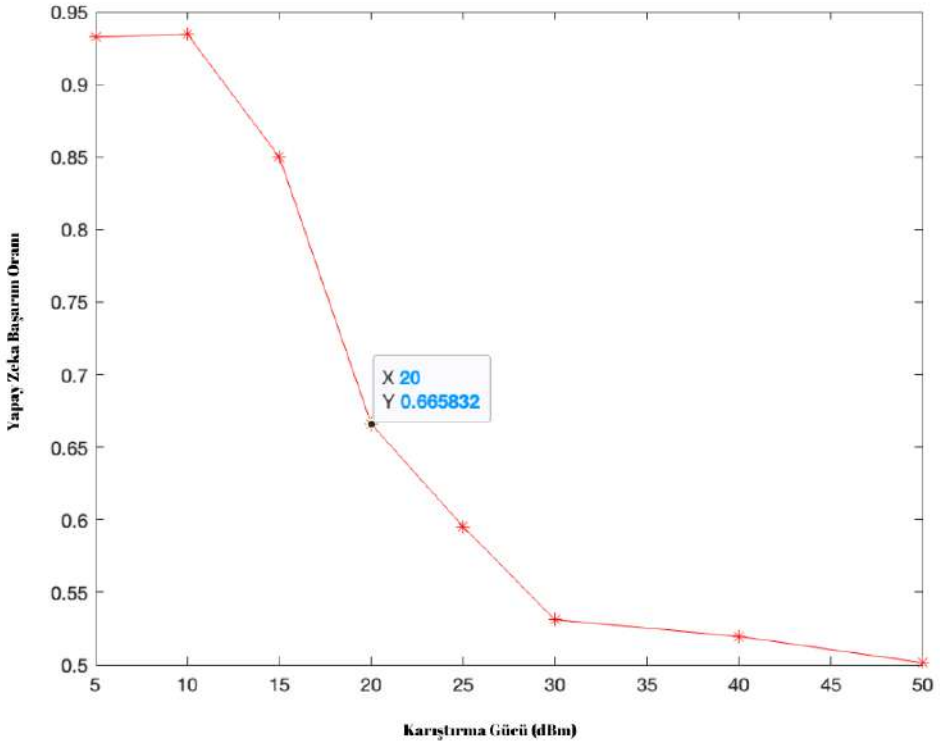
Karıştırıcının etkisi altında, özellikle 20 dB gürültü seviyesinden sonra, sınıflandırma performansında ciddi bir düşüş gözlemlenmiştir. Bu seviyedeki karışıklık matrisi **Şekil 4.1**'de sunulmuştur. Bu matris temelinde yapılan değerlendirmeler aşağıdaki gibidir:

1. **İnsan Sinyali Olduğunda**: Sınıflandırıcı, insan sinyallerini sadece %14,42 oranında doğru bir şekilde tespit edebilmiştir. Bu düşük başarı oranı, karıştırıcının insan sinyalleri üzerindeki olumsuz etkisini açıkça göstermektedir. İnsan sinyallerinin büyük bir kısmı, karıştırıcı etkisiyle yanlış sınıflandırılmış veya gürültü olarak algılanmıştır. Bu durum, sistemin insan hedeflerini tespit etme kabiliyetinin karıştırıcı etkisi altında ciddi şekilde azaldığını göstermektedir.

2. **Gürültü Sinyali Olduğunda**: Gürültü sinyallerinin doğru sınıflandırma oranı %99,79 olarak elde edilmiştir. Bu yüksek başarı oranı, sınıflandırıcının gürültü sinyallerini karıştırıcı etkisi altında bile doğru bir şekilde tanımlayabildiğini göstermektedir. Bu, gürültü sinyallerinin özelliklerinin karıştırıcıdan nispeten daha az etkilendiğini ve sınıflandırıcının bu sinyalleri başarılı bir şekilde ayırt edebildiğini işaret etmektedir.
3. **Hayvan Sinyali Olduğunda**: Hayvan sinyallerinin doğru sınıflandırma oranı %96,99 olarak belirlenmiştir. Sınıflandırıcı, hayvan sinyallerini karıştırıcı etkisi altında bile yüksek bir doğrulukla tespit edebilmiştir. Bu, hayvan sinyallerinin karakteristik özelliklerinin karıştırıcıdan daha az etkilendiğini ve sistemin hayvan hedeflerini tespit etmede daha başarılı olduğunu göstermektedir.
4. **Boş Ortamda**: Boş ortam sinyallerinin doğru sınıflandırma oranı %55,11 olarak saptanmıştır. Bu orta düzey başarı oranı, karıştırıcının boş ortam sinyallerini etkilediğini ve sınıflandırıcının bu sinyalleri bazen yanlış sınıflandırdığını göstermektedir. Boş ortam sinyallerinin karıştırıcı etkisi altında diğer sınıflarla karıştırılma olasılığı artmış ve bu da sistemin genel performansını olumsuz etkilemiştir.

Sonuçlar incelendiğinde, özellikle insan sinyallerinin karıştırıcı etkisi altında büyük oranda yanlış sınıflandırıldığı ve boş ortamda dahi hatalı sınıflandırmaların yüksek olduğu görülmüştür. Örneğin, insan sinyallerinin hayvan olarak sınıflandırılma oranı %44,88 gibi yüksek bir seviyeye ulaşmıştır. Bu bulgular, 20 dB seviyesindeki karıştırıcı etkisinin radar sisteminin kullanılabilirliğini ciddi şekilde azalttığını göstermektedir.

Sonuç olarak, saldırılara dirençli yapay zekâ tabanlı bir sınıflandırıcı geliştirilmiştir. Bu sınıflandırıcı, insan ve hayvan ayrımını başarılı bir şekilde gerçekleştirmekle kalmayıp, aynı zamanda karıştırma saldırısı altında olup olmadığını da tespit edebilmektedir. Bu özellik, sistemin güvenilirliğini ve saldırılara karşı direncini önemli ölçüde artırmaktadır. Yapay zekânın karıştırıcı varlığını tespit etme etkinliği **Şekil 4.7**'de gösterilmiştir.



Şekil 4.2: Karıştırıcı etkisi altında sınıflandırma bozulması

4.2. KARIŞTIRMA DİRENÇLİ YÖNTEMİNİN BAŞARIMI

Bu çalışma, doppler radar tabanlı insan sınıflandırma sistemlerinin güvenliğini artırmak ve aldatma (*spoofing*) saldırılarına karşı dirençli hale getirmek amacıyla önemli bir adım olarak değerlendirilebilir. Elde edilen bulgular, bu tür radar sistemlerinin güvenlik açıklarını anlamak ve gidermek için kritik öneme sahiptir ve gelecekteki araştırmalar için sağlam bir temel oluşturacaktır. Ayrıca, bu çalışma, benzer güvenlik tehditlerine maruz kalan diğer radar ve algılama sistemleri için de yol gösterici olabilir.

Çalışmada temel olarak kullanılan yöntem, toplanan orijinal verilerin üzerine farklı gürültü seviyelerinde karıştırma verilerinin uygulanması ve bu şekilde zenginleştirilmiş yeni bir veri setinin oluşturulmasıdır. Bu genişletilmiş veri seti, çeşitli karıştırma koşullarını temsil eden örnekleri içermektedir. Daha sonra, bu yeni veri seti kullanılarak yeniden eğitilen bir sınıflandırıcının, gürültü ve karıştırma etkisi altında daha yüksek bir performans sergilemesi beklenmektedir. Bu yaklaşım, modelin genelleme yeteneğini artırarak, gerçek

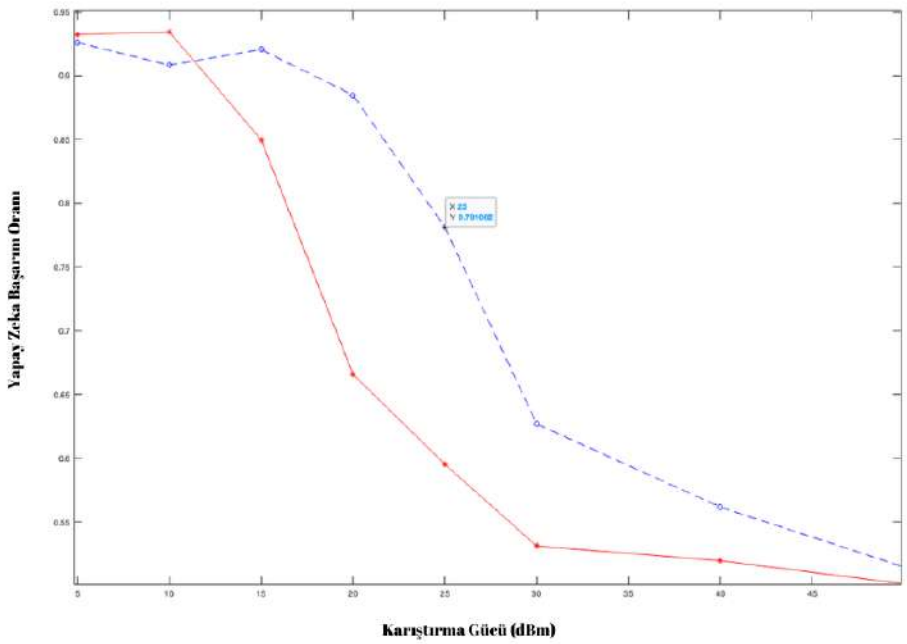
dünya koşullarında karşılaşılabilecek saldırılara karşı daha dirençli olmasını sağlamayı amaçlamaktadır.

Beklendiği gibi, ortalama doğru sınıflandırma oranlarında belirgin bir artış gözlemlenmiştir. Ancak, ilginç bir şekilde, düşük gürültü seviyelerinde sınıflandırıcının performansında hafif bir düşüş tespit edilmiştir. Bu durumun, veri setinin entropisinin artmasından kaynaklandığı düşünülmektedir. Veri setinin belirli verilerle zenginleştirilmesi sırasında, entropinin aşırı yükseltilmemesi gerektiği önemli bir faktör olarak ortaya çıkmaktadır. Örneğin, sınıflandırıcımız kapsamında, "gürültü" ve "boş" durumlarının ayrı birer sınıf olarak ele alınmasının, teorik çalışmamızın pratik uygulamalarında daha verimli olacağını düşünmekteyiz. Bu nedenle, çalışmamızda birinci sınıfı "boş" durum, ikinci sınıfı ise "gürültü" durum olarak tanımladık. Ancak, veri zenginleştirme aşamasında, karıştırıcı gürültüsü hem diğer sınıflara hem de "boş" durumu temsil eden sınıflara uygulanmıştır. Bu durum, gerçek veri seti içinde özellikle düşük gürültü seviyelerinde ayrıştırılması zor olan nesnelerin oluşmasına yol açmıştır. Dolayısıyla, karşı önlemin dahil edildiği sınıflandırıcının düşük gürültü seviyelerinde daha düşük performans göstermesini, veri seti entropisinin artmasına bağlamaktayız.

Bunun yanı sıra, yeni oluşturulan dirençli sınıflandırıcı, 5 dB'den daha fazla bir karıştırma direnci sağlamıştır. Bu bağlamda, elde edilen girişim direncinin oldukça başarılı olduğu söylenebilir. Örneğin, girişim direnci olmadan 20 dB karıştırma altında %66,58'e düşen sınıflandırma doğruluğu, dirençli model ile 25 dB gürültü seviyesinde %78,10'a yükselmiştir. Bu sonuçlar, sınıflandırıcının karıştırma etkisine karşı önemli ölçüde dayanıklılık kazandığını göstermektedir. Detaylı performans analizleri ve karşılaştırmalar için **Şekil 4.3** incelenebilir.

4.3. KARIŞTIRMA TESPİT YÖNTEMİNİN BAŞARIMI

Karıştırma saldırısının bir kanalda yapılıp yapılmadığını belirlemek amacıyla eğitilen sınıflandırıcımızın performansı, farklı gürültü seviyelerine bağlı olarak değişkenlik göstermektedir. Bu çalışmada gerçekleştirilen sınıflandırma,



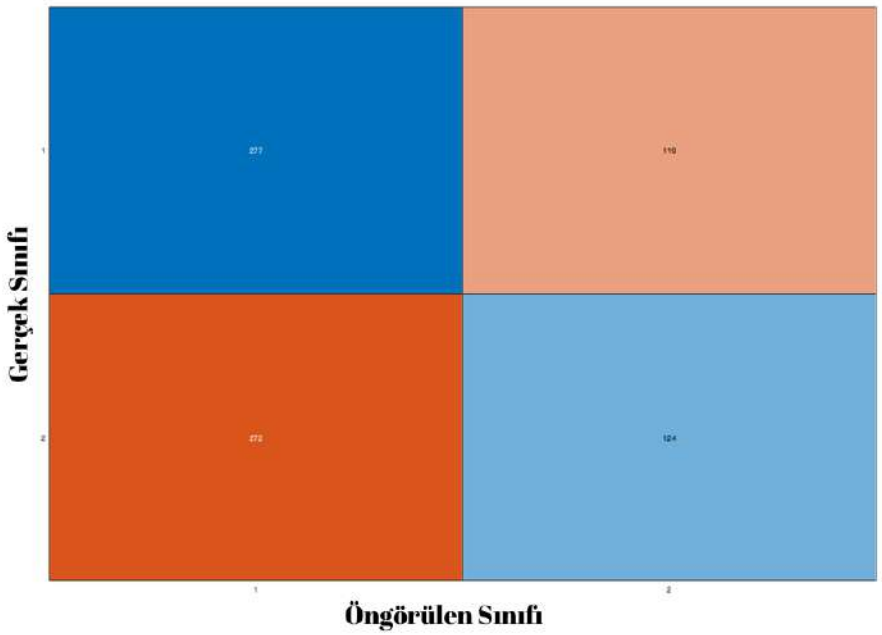
Şekil 4.3: Karıştırıcı Önlem Etkinliği

rastgele seçilen arka plan, gürültü, hayvan ve insan verilerinden oluşan bir veri kümesinin üzerine karıştırma uygulanmış veya uygulanmamış verilerin eklenmesiyle oluşturulmuştur. Sistemin karşılaştığı zorluklardan biri, karıştırma uygulanmamış veri kümesindeki örneklerin %25'inin, hedefin radara çok yakın olduğu durumları simüle eden gürültü verilerinden oluşmasıdır. Bu veriler, kullanılan karıştırıcının verilerine oldukça benzemekte ve dolayısıyla sınıflandırıcının performansını olumsuz yönde etkilemektedir. Bu nedenle, ilgili veri setinde yanlış pozitif sonuçların elde edilmesi doğal bir durum olarak değerlendirilmiştir.

10 dB Gürültü Seviyesindeki Performans

Sınıflandırıcımız, 10 dB gürültü seviyesinde %50,63 başarı oranı sağlamıştır. Karmaşıklık matrisi incelendiğinde, sınıflandırıcının etkinliğinin yetersiz olduğu görülmektedir. Bunun temel sebebi, 10 dB gürültü seviyesinin oldukça düşük bir gürültü olması ve sinyal seviyesine kıyasla yetersiz kalmasıdır. Düşük gürültü seviyelerinde karıştırma etkisinin belirgin olmaması, sınıflandırıcının

karıştırmayı tespit etme kabiliyetini azaltmaktadır. Bu durum **Şekil 4.4**'de gösterilmiştir.



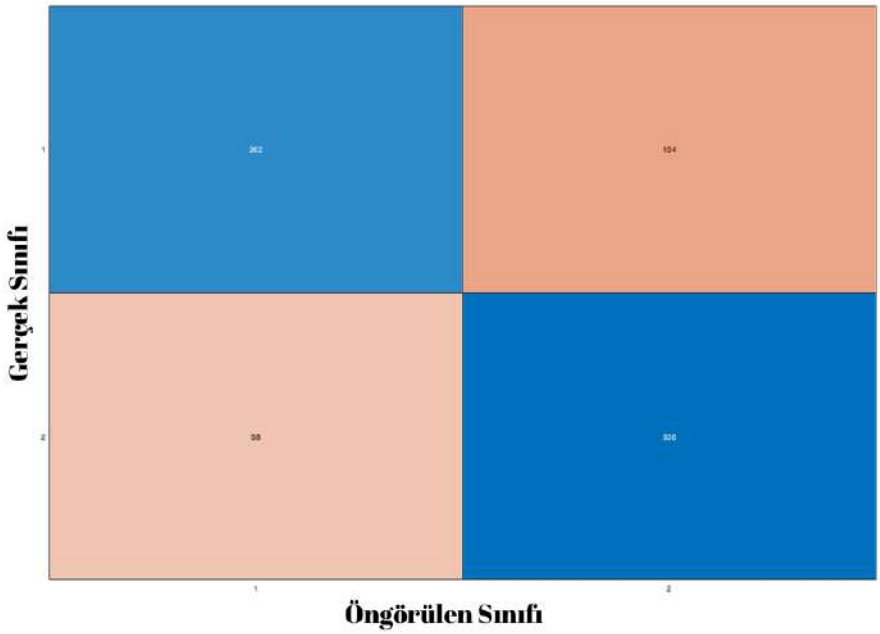
Şekil 4.4: 10 dB'de Karıştırıcı Tespit Etkinliği

25 dB Gürültü Seviyesindeki Performans

25 dB karıştırma seviyesi için, oldukça başarılı sayılabilecek bir sınıflandırıcı elde edilmiştir. Karıştırıcının bulunduğu durumlarda, saldırganın tespiti %88,30 başarı oranıyla mümkün olmuştur. Saldırganın tespit edilmesi bakımından bu sonuçlar oldukça olumludur. Ancak, daha önce bahsedilen doğal gürültünün de veri setinde bulunması fenomeni nedeniyle, genel başarı oranı %75,75'e düşmüştür. Bu düşüş, sınıflandırıcının yanlış pozitif ve yanlış negatif oranlarındaki artıştan kaynaklanmaktadır. Bu durum **Şekil 4.5**'de gösterilmiştir.

50 dB Gürültü Seviyesindeki Performans

50 dB karıştırma seviyesinde, sınıflandırıcımız tüm saldırganları %100 başarı oranıyla tespit edebilmiştir. Bu yüksek başarı, karıştırma etkisinin yüksek gürültü seviyelerinde daha belirgin hale gelmesiyle açıklanabilir. Ancak, doğal

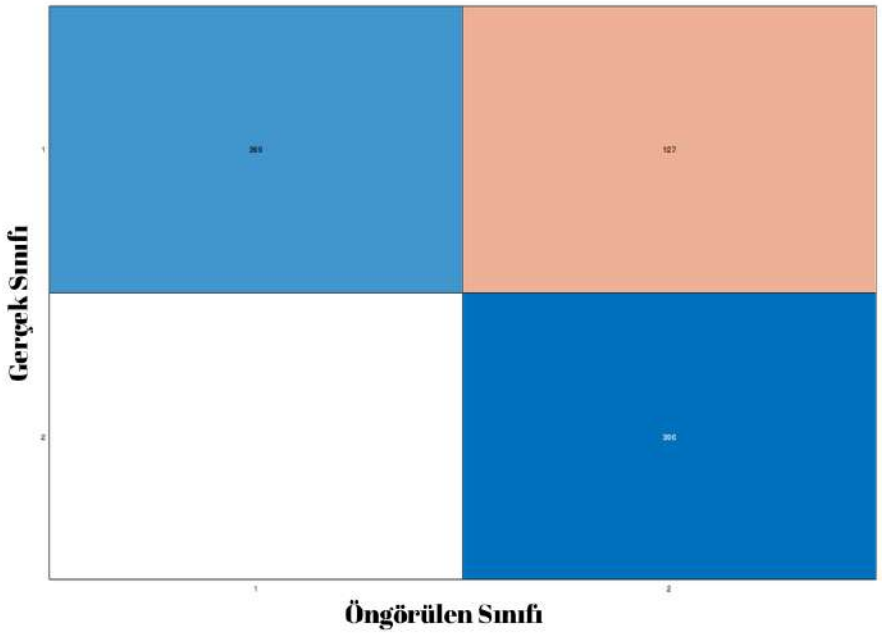


Şekil 4.5: 25 dB'de Karıştırıcı Tespit Etkinliği

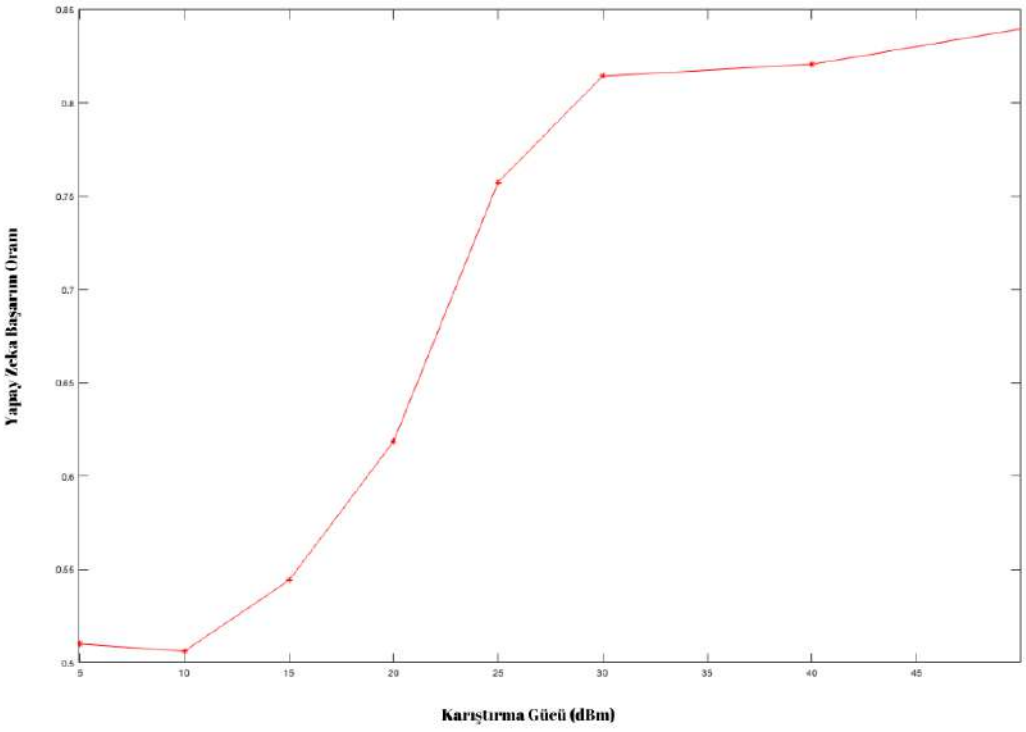
gürültünün veri setinde bulunması nedeniyle, genel başarı oranı %83,96 olarak hesaplanmıştır. Bu durum, yüksek gürültü seviyelerinde bile doğal gürültünün sınıflandırıcı performansını bir miktar olumsuz etkilediğini göstermektedir. **Şekil 4.6**'de bu sonuçlar detaylı olarak sunulmuştur.

4.4. GENEL DEĞERLENDİRME

Şekil 4.7'de gösterildiği üzere, 25 dB gürültü seviyesinden sonra radar üzerinde bir karıştırma saldırısının yapılıp yapılmadığını güvenilir bir şekilde tespit etmek mümkün olmaktadır. Bu durum, karıştırma etkisinin belirgin hale geldiği ve sınıflandırıcının performansının arttığı bir eşiği göstermektedir. Ayrıca, **Şekil 4.3**'de gösterildiği gibi, karıştırıcıya dayanıklı sınıflandırıcının başarım oranlarının kritik oranda düştüğü noktada, karıştırıcı tespit sisteminin etkinliği artmaktadır. Bu bulgu, karıştırıcı tespit sistemi ile karıştırıcıya dayanıklı yapay zekânın tandem olarak kullanıldığı güvenilir bir sistemin geliştirilmesinin mümkün olabileceğini göstermektedir.



Şekil 4.6: 50 dB'de Karıştırıcı Tespit Etkinliği



Şekil 4.7: Karıştırıcı Tespit Edebilme Oranı

5. TARTIŞMA

Bu tez çalışması kapsamında, temel olarak bir radar sisteminde karıştırma saldırılarının algoritmik yöntemlerle tespitinin imkansız olduğu, ancak sezgisel yöntemlerle tespit edilebileceği iddia edilmiştir. Bu iddia, öncelikle matematiksel olarak temellendirilmiş ve ardından deneysel olarak doğrulanmıştır.

Bu çalışmanın en önemli katkılarından biri, özgün bir CW radar tabanlı veri toplama cihazı ve CW radar jammer geliştirilmesidir. Bu cihazlar, gerçek dünya senaryolarını simüle ederek, karıştırma saldırıları ve karşı önlemler üzerine yapılan araştırmalara önemli bir katkı sağlayacaktır.

Yukarıda sayılanın yanında tez kapsamında toplanan veri seti literatürde görülen en geniş veri setlerinden birisi olarak sayılabilir. Daha önceden toplanan veri setlerinde inek [16], at [14], koyun [16], köpek [28] gibi hayvanların verileri toplanmıştır. Bazı çalışmalarda vahşi hayvanların da verileri toplandığı söylenebilir. Fakat geyik, cüce domuz, kurt, keçi, ceylan gibi hayvanların verileri ilk defa toplanmıştır. Toplanan özgün veri seti, bu alandaki gelecekteki çalışmalar için değerli bir kaynak olacaktır.

Tablo 5.1: Cao'nun yayınındaki insan ve köpek sınıflandırma oranları

Sınıflandırma Tekniği	**Doğru İnsan**	**Yanlış İnsan**	**Doğru Köpek**	**Yanlış Köpek**
DCNN	%98	%1	%99	% 2
SVM	%92	%20	%80	% 8
NB	%80	%25	%75	% 20
SVM-NB Fusion	%93	%14	%86	% 7

Çalışma kapsamında insan hayvan ayrımı yapan bir yapay zeka geliştirilmiştir. Bu bakımdan literatürde yapılan pek çok çalışmaya da yayın kapsamında değinilmiştir. Bu çalışmalardan en başarılılarından birisi Cao ve diğ. [28] tarafından yapılmıştır. Cao'nun çalışmasında alınan değerler **Tablo 5.1** da verilmiştir. Bu çalışmada kullanılan sınıflandırıcı başarım bakımından

literatürdeki alternatifleri ile benzer bir başarım oranı olan %94,74 ile çalışmıştır. Bu bakımdan gerçeklenen sınıflandırıcının geçerli bir sınıflandırıcı olduğu söylenebilir. Detaylı karşıklık matrisi **Şekil 3.5**'te gösterilmiştir.

Ayrıca, bu çalışmada geliştirilen karıştırıcı tespit sistemi ve karıştırıcıya dayanıklı yapay zeka modelinin birlikte kullanımı, radar tabanlı güvenlik sistemlerinin güvenilirliğini önemli ölçüde artırma potansiyeline sahiptir. Bu yaklaşım, [62]'in önerdiği radar sinyal işleme tekniklerini tamamlayıcı niteliktedir. Bu yöntemler, geleneksel algoritmik yaklaşımların yetersiz kaldığı durumlarda bile başarılı sonuçlar vermiştir. Özellikle, 25 dB ve üzeri gürültü seviyelerinde karıştırma saldırılarının güvenilir bir şekilde tespit edilebilmesi, bu yaklaşımın pratik uygulamalardaki potansiyelini göstermektedir.

Geliştirdiğimiz sistemin pratik uygulamalardaki potansiyeli, [77]'in insan aktivite tanıma çalışmasıyla paralellik göstermektedir. Kim ve ark. çalışmasında kullanılan mikro-Doppler özellik çıkartmak için 0.6, 1.1, 1.5, 2.1, 2.6, ve 3.0 sn'lik radar izlerine dayanırken. Bizim çalışmamızda standart 1.0 sn'lik radar izi kullanımı ile benzer başarımda sınıflandırma sağlanmıştır. 1.0sn olan pencere aralığında kim ve arkadaşlarının çalışması %86,5 başarım oranına sahipken bu çalışma kapsamında **Şekil 3.5** ile gösterildiği üzere %94,74 başarıma ulaşılabilmiştir. Bu bakımdan var olan literatüre katkı yapılmıştır.

Ayrıca **Şekil 5.1**'de sunulan ortam güvenliği uygulaması akış diyagramı, bu çalışmanın sonuçlarının nasıl entegre edilebileceğini göstermektedir. Bu sistem, hem insan/hayvan ayrımı yapabilen hem de karıştırma saldırılarını tespit edebilen iki farklı sınıflandırıcıyı birleştirerek, güvenlik uygulamalarında yeni bir standart oluşturma potansiyeline sahiptir.Gelecekteki çalışmalarda, [61]'un önerdiği çoklu sensör füzyon teknikleri ile bizim geliştirdiğimiz karıştırıcıya dayanıklı sınıflandırma yöntemlerinin birleştirilmesi, radar tabanlı güvenlik sistemlerinin performansını daha da artırabilir.

Doktora çalışmasının bir sonraki aşaması radara spoofing saldırısı yapılması olmuştur. Bu saldırıyı saldırga cihazın 5 dB, 10 dB, 15 dB 20 dB, 25 dB, 30dB, 40 dB, 50 dB gürültülerde yapılması ile sağlanmıştır. Fioranelli ve diğ. [60] 1 dB, 5dB, 10dB, 15dB, 20 dB gürültü kullanırken [61]. 0 - 64 dB aralığında saldırı

yapmıştır. Bizim sistemimizde 50 dB de maksimum karıştırma oranına erişildiği için daha yüksek gürültü seviyesinin araştırılmasına ihtiyaç görülmemiştir.

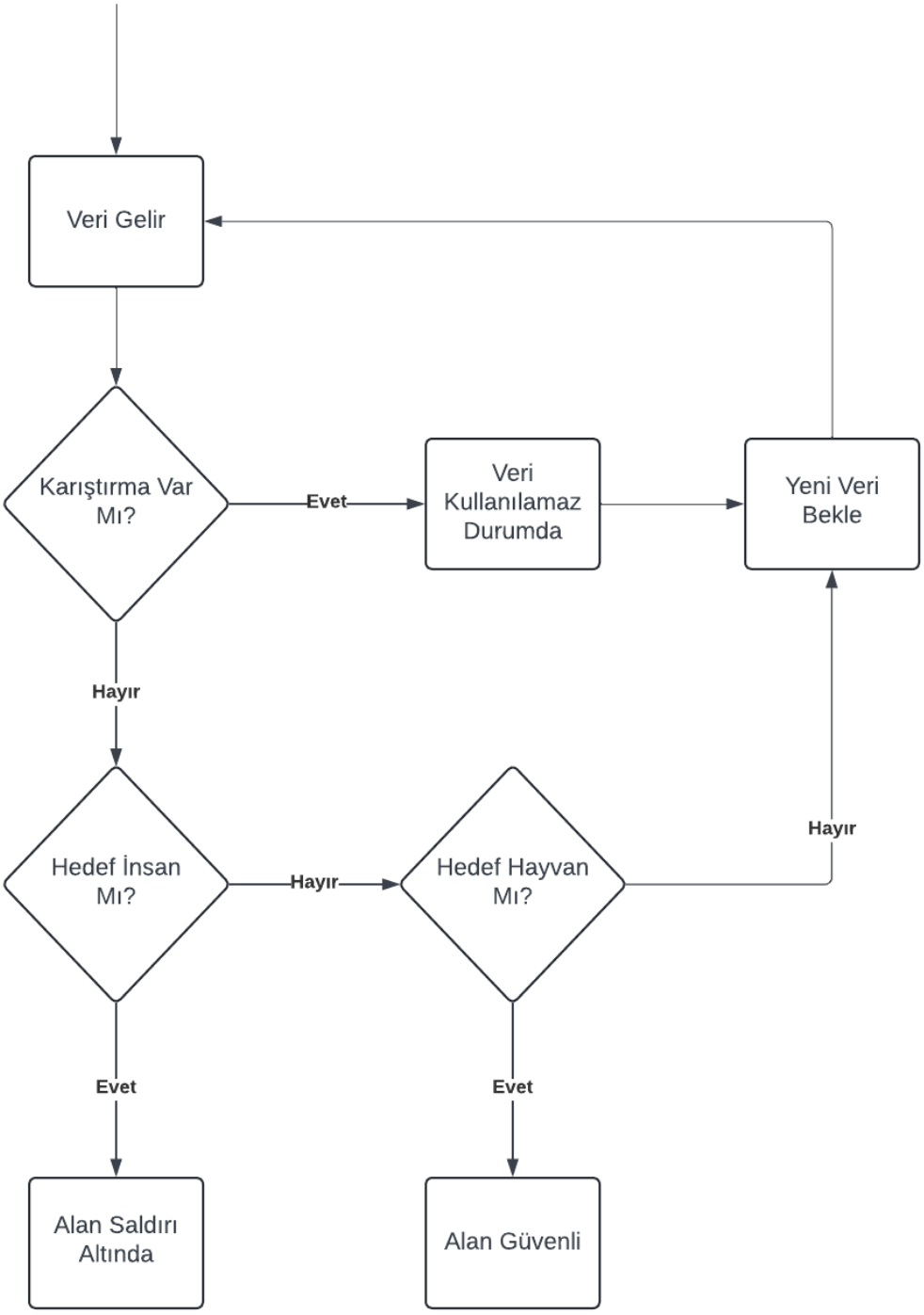
Bununla birlikte, geliştirilen karıştırıcıya dayanıklı sınıflandırıcının performansı da dikkat çekicidir. 20 dB gürültü seviyesinde, saldırı direnci olmadan %66,58 olan başarım oranının, saldırı direnci ile %88,47'ye yükselmesi, önerilen yöntemin etkinliğini açıkça ortaya koymaktadır. Bu sonuç, literatürdeki benzer çalışmaların elde ettiği en yüksek başarım oranlarını aşmakta ve yöntemimizin üstünlüğünü göstermektedir.

Ancak, çalışmamızın bazı sınırlamaları da bulunmaktadır. Örneğin, deneyler belirli bir CW radar sistemi ve sınırlı sayıda karıştırma saldırısı senaryosu üzerinde gerçekleştirilmiştir. Bu nedenle, sonuçların genelleştirilebilirliği konusunda dikkatli olunmalıdır. Gelecekteki çalışmalar, farklı radar sistemleri ve daha geniş bir karıştırma saldırısı yelpazesi üzerinde gerçekleştirilerek bu sınırlamaların üstesinden gelebilir.

Saldırı yapılmasının ardından saldırıya dirençli yapay zeka tabanlı sınıflandırıcı, geliştirilmiştir. Bu geliştirilen sınıflandırıcının performansı **Şekil 4.3**'de gösterilmiştir. Dirençli yapay zekanın 20dB'de direnç olmadığı halde %66,58'de iken saldırı direnci ile birlikte performansı %88,47 olmuştur. Bu dirençli sistem 20 dB gürültü seviyesi için literatürde bilinen en yüksek seviye olan [60]'in elde ettiği başarım olan %85,01'den daha yüksek olmuştur.

Geliştirilen saldırıya dirençli yapay zeka tabanlı sınıflandırıcı, hem insan/hayvan ayrımı yapabilme hem de karıştırma saldırılarını tespit edebilme yeteneği ile mevcut yöntemlere kıyasla önemli bir ilerleme sunmaktadır. Bu sınıflandırıcı, radar sistemlerinin güvenliğini artırmak ve karıştırma saldırılarına karşı daha etkili savunma mekanizmaları geliştirmek için kullanılabilir. Sınıflandırıcının çeşitli gürültü seviyelerinde tespit edebilme düzeyine dair veriler **Şekil 4.7**'de bulunabilir.

Sonuç olarak geliştirilen yapay zekaları kullanarak ortam güvenliği uygulamalrında kullanılabilecek bir orijinal uygulama akış diyagramı da **Şekil 5.1**'de verilmiştir. Bu akış diyagramını kullanan bir sisitemin



Şekil 5.1: Ortam güvenliği uygulaması akış diyagramı.

tezimiz kapsamında geliştirilen 2 sınıflandırıcıyı da kullanması gerekecektir. Sınıflandırıcıların koordinasyonu sayesinde literatürde daha önce bulunmayan yüksek güvenilirlikte bir ortam güvenliği uygulaması sağlanmış olacaktır.

6. SONUÇ VE ÖNERİLER

Bu tez çalışmasında, doppler radar tabanlı insan sınıflandırma sistemlerine yönelik karıştırma (jamming) saldırılarının tespiti ve hafifletilmesi üzerine kapsamlı bir araştırma gerçekleştirilmiştir. Elde edilen sonuçlar, belirli bir CW radar sistemi ve sınırlı sayıda karıştırma saldırısı senaryosu üzerinde gerçekleştirilen deneylere dayanmaktadır. Bu nedenle, bulguların genelleştirilebilirliği sınırlı olabilir; gelecekteki çalışmalar farklı radar sistemleri ve daha geniş bir karıştırma saldırısı yelpazesi üzerinde gerçekleştirilebilir.

Literatür, yürüyüş analizinde bacak ve kol hareketleri gibi özelliklere odaklanmıştır. Bu özellikler, cinsiyet, boy ve kimlik gibi insan özelliklerinin ayrımını sağlar. Güvenlik uygulamalarında, yürüyüş analizi yüz tanıma olmadan şüphelilerin tanımlanmasına yardımcı olabilir.

Bu tür sensörlerin, özellikle güvenlik alanında yaygın kullanımıyla, bu sensörlere yönelik siber saldırıların artacağı öngörülmektedir. Ancak, literatürde bu alandaki yayınların sınırlı ve tek boyutlu olduğu gözlemlenmiştir [47]. İnsanları tespit eden sistemlere insanları araç veya hayvan olarak tanıtan çalışmalara rastlanmamaktadır. Bu nedenle, insan tanımlaması yapan sistemler için yeni bir tür aldatma saldırısının geliştirilmesi gerektiği görülmüştür.

Çalışmamız kapsamında çeşitli hayvan tiplerini içeren bir radar izi veri tabanı oluşturulmuştur. Bu veri tabanı kullanılarak hayvan türlerinin sınıflandırılması nispeten keşfedilmemiştir. Böyle bir araştırma, doğal yaşam alanlarında çeşitli türlerin izlenmesi ve yönetimi için verimli ve müdahaleci olmayan yöntemler sağlayarak, vahşi yaşam koruma çalışmalarına büyük fayda sağlayabilir. Hayvan türleri arasında ayrım yaparak, korumacılar farklı hayvanların dağılımı, popülasyon dinamikleri ve davranışları hakkında değerli içgörüler elde edebilirler.

Bu çalışmada kullanılan sezgisel yöntemlerin performansı, daha gelişmiş saldırı teknikleri karşısında da değerlendirilmelidir. Saldırganlar, bu yöntemleri yanıltmak için daha karmaşık ve adaptif stratejiler kullanabilirler. Bu nedenle, gelecekteki araştırmalar, daha gelişmiş saldırı senaryolarını dikkate almalı ve sezgisel yöntemlerin bu tür saldırılara karşı etkinliğini değerlendirmelidir.

Sonuç olarak, bu tez çalışması doppler radar tabanlı insan sınıflandırma sistemlerine yönelik karıştırma saldırılarının tespiti ve hafifletilmesi konusunda önemli bir adım atmıştır. Elde edilen sonuçlar, sezgisel yöntemlerin bu tür saldırıların tespitinde ve sistemlerin güvenliğinin artırılmasında umut verici bir yaklaşım olduğunu göstermektedir. Bu çalışma, gelecekteki araştırmalar için sağlam bir temel oluşturmakta ve radar sistemlerinin güvenliğini artırmak için yeni yöntemlerin geliştirilmesine katkı sağlayacaktır.

KAYNAKLAR

[1]. Tahmoush, D. and Silvious, J. 2009. Remote detection of humans and animals. In *2009 ieee applied imagery pattern recognition workshop (AIPR 2009)*, pages 1–8. IEEE.

[2]. Lai, C.-P., Narayanan, R., and Culkowski, G. 2006. Through wall surveillance using ultrawideband random noise radar. Technical report.

[3]. Lai, C.-P. 2007. *Through wall surveillance using ultrawideband random noise radar*. The pennsylvania state university.

[4]. Tahmoush, D. and Silvious, J. 2009. Angle, elevation, prf, and illumination in radar microdoppler for security applications. In *2009 ieee antennas and propagation society international symposium*, pages 1–4. IEEE.

[5]. Bryan, J., Kwon, J., Lee, N., and Kim, Y. 2012. Application of ultra-wide band radar for classification of human activities. *Iet radar, sonar & navigation*, 6(3):172–179. IET.

[6]. Gürbüz, S. Z., Tekeli, B., Yüksel, M., Karabacak, C., Gürbüz, A. C., and Guldogan, M. B. 2013. Importance ranking of features for human micro-doppler classification with a radar network. In *Proceedings of the 16th international conference on information fusion*, pages 610–616. IEEE.

[7]. Narayanan, R. M. and Zenaldin, M. 2015. Radar micro-doppler signatures of various human activities. *Iet radar, sonar & navigation*, 9(9):1205–1215. IET.

[8]. Li, C. 2018. Walking gait measurement and gait parameters extraction. PhD thesis, The University of Mississippi.

[9]. Rahman, H. 2019. *Fundamental principles of radar*. CRC Press.

[10]. Fioranelli, F., Ritchie, M., and Griffiths, H. 2015. Aspect angle dependence and multistatic data fusion for micro-doppler classification of armed/unarmed personnel. *Iet radar, sonar & navigation*, 9(9):1231–1239. Wiley Online Library.

[11]. Fioranelli, F., Ritchie, M., and Griffiths, H. 2015. Analysis of polarimetric multistatic human micro-doppler classification of armed/unarmed personnel. In *2015 ieee radar conference (radarcon)*, pages 0432–0437. IEEE.

[12]. Fioranelli, F., Ritchie, M., and Griffiths, H. 2016. Centroid features for classification of armed/unarmed multiple personnel using multistatic

human micro-doppler. *Iet radar, sonar & navigation*, 10(9):1702–1710. Wiley Online Library.

[13]. Patel, J. S., Fioranelli, F., Ritchie, M., and Griffiths, H. 2018. Multistatic radar classification of armed vs unarmed personnel using neural networks. *Evolving systems*, 9(2):135–144. Springer.

[14]. Shrestha, A., Le Kernec, J., Fioranelli, F., Marshall, J. F., and Voute, L. 2017. Gait analysis of horses for lameness detection with radar sensors. IET.

[15]. Shrestha, A., Loukas, C., Le Kernec, J., Fioranelli, F., Busin, V., Jonsson, N., King, G., Tomlinson, M., Viora, L., and Voute, L. 2018. Animal lameness detection with radar sensing. *Ieee geoscience and remote sensing letters*, 15(8):1189–1193. IEEE.

[16]. Fioranelli, F., Li, H., Le Kernec, J., Busin, V., Jonsson, N., King, G., Tomlinson, M., and Viora, L. 2019. Radar-based evaluation of lameness detection in ruminants: preliminary results. In *2019 ieee mtt-s international microwave biomedical conference (imbioc)*, volume 1, pages 1–4. IEEE.

[17]. Shruthi, N., Mathur, P., and Kurup, D. G. 2018. Performance of ultra wideband (uwb) pulsed doppler radar for heart rate and respiration rate monitoring in noise. In *2018 international conference on advances in computing, communications and informatics (ICACCI)*, pages 722–725. IEEE.

[18]. Liu, Z., Sui, J., Wei, Z., and Li, X. 2018. A sparse-driven anti-velocity deception jamming strategy based on pulse-doppler radar with random pulse initial phases. *Sensors*, 18(4):1249. Multidisciplinary Digital Publishing Institute.

[19]. Li, T., Wang, Z., and Liu, J. 2020. Evaluation method for impact of jamming on radar based on expert knowledge and data mining. *Iet radar, sonar & navigation*, 14(9):1441–1450. Wiley Online Library.

[20]. Bhattacharya, A. and Vaughan, R. 2020. Deep learning radar design for breathing and fall detection. *Ieee sensors journal*, 20(9):5072–5085. IEEE.

[21]. Li, H., Shrestha, A., Heidari, H., Le Kernec, J., and Fioranelli, F. 2019. Bi-lstm network for multimodal continuous human activity recognition and fall detection. *Ieee sensors journal*, 20(3):1191–1201. IEEE.

[22]. Li, H. 2021. Multimodal radar sensing for ambient assisted living. PhD thesis, University of Glasgow.

[23]. Vandersmissen, B., Knudde, N., Jalalvand, A., Couckuyt, I., Bourdoux, A., De Neve, W., and Dhaene, T. 2018. Indoor person identification using a low-power fmcw radar. *Ieee transactions on geoscience and remote sensing*, 56(7):3941–3952. IEEE.

[24]. Vandersmissen, B., Knudde, N., Jalalvand, A., Couckuyt, I., Dhaene, T., and De Neve, W. 2020. Indoor human activity recognition using high-dimensional sensors and deep neural networks. *Neural computing and applications*, 32(16):12295–12309. Springer.

[25]. de Jong, R. J., de Wit, J. J., and Uysal, F. 2021. Classification of human activity using radar and video multimodal learning. *Iet radar, sonar and navigation*. Institution of Engineering and Technology.

[26]. Gurbuz, S. Z. and Amin, M. G. 2019. Radar-based human-motion recognition with deep learning: Promising applications for indoor monitoring. *Ieee signal processing magazine*, 36(4):16–28. IEEE.

[27]. Islam, S. M., Sylvester, A., Orpilla, G., and Lubecke, V. M. 2020. Respiratory feature extraction for radar-based continuous identity authentication. In *2020 ieee radio and wireless symposium (RWS)*, pages 119–122. IEEE.

[28]. Cao, P., Xia, W., and Li, Y. 2018. Classification of ground targets based on radar micro-doppler signatures using deep learning and conventional supervised learning methods. *Radioengineering*, 27(3):835–845.

[29]. Li, G., Zhang, S., Fioranelli, F., and Griffiths, H. 2018. Effect of sparsity-aware time–frequency analysis on dynamic hand gesture classification with radar micro-doppler signatures. *Iet radar, sonar & navigation*, 12(8):815–820. Wiley Online Library.

[30]. Saho, K., Inuzuka, K., and Shioiri, K. 2020. Person identification based on micro-doppler signatures of sit-to-stand and stand-to-sit movements using a convolutional neural network. *Ieee sensors letters*, 4(3):1–4. IEEE.

[31]. Gurbuz, S. Z., Clemente, C., Balleri, A., and Soraghan, J. J. 2017. Micro-doppler-based in-home aided and unaided walking recognition with multiple radar and sonar systems. *Iet radar, sonar & navigation*, 11(1):107–115. IET.

[32]. Gao, X., Xing, G., Roy, S., and Liu, H. 2019. Experiments with mmwave automotive radar test-bed. In *2019 53rd asilomar conference on signals, systems, and computers*, pages 1–6. IEEE.

[33]. Severino, J. V. B., Zimmer, A., Brandmeier, T., and Freire, R. Z. 2019. Pedestrian recognition using micro doppler effects of radar signals based on machine learning and multi-objective optimization. *Expert systems with applications*, 136:304–315. Elsevier.

[34]. Lee, S., Yoon, Y.-J., Lee, J.-E., and Kim, S.-C. 2017. Human–vehicle classification using feature-based svm in 77-ghz automotive fmcw radar. *Iet radar, sonar & navigation*, 11(10):1589–1596. Wiley Online Library.

[35]. Xu, R., Zhu, Y., Lu, K., and An, H. 2022. Object detection of millimeter wave radar based on computer vision. In *2022 4th international conference on advances in computer technology, information science and communications (ctisc)*, pages 1–8. IEEE.

[36]. Ulrich, M., Gläser, C., and Timm, F. 2021. Deepreflecs: Deep learning for automotive object classification with radar reflections. In *2021 ieee radar conference (radarconf21)*, pages 1–6. IEEE.

[37]. Rizik, A., Randazzo, A., Vio, R., Delucchi, A., Chible, H., and Caviglia, D. D. 2020. Low-cost fmcw radar human-vehicle classification based on transfer learning. In *2020 32nd international conference on microelectronics (icm)*, pages 1–4. IEEE.

[38]. Shenoy, J., Liu, Z., Tao, B., Kabelac, Z., and Vasisht, D. 2022. Rf-protect: privacy against device-free human tracking. In *Proceedings of the acm sigcomm 2022 conference*, pages 588–600.

[39]. Chipengo, U., Sligar, A. P., Canta, S. M., Goldgruber, M., Leibovich, H., and Carpenter, S. 2021. High fidelity physics simulation-based convolutional neural network for automotive radar target classification using micro-doppler. *Ieee access*, 9:82597–82617. IEEE.

[40]. Hämäläinen, M., Mucchi, L., Caputo, S., Biotti, L., Ciani, L., Marabissi, D., and Patrizi, G. 2021. Ultra-wideband radar-based indoor activity monitoring for elderly care. *Sensors*, 21(9):3158. Multidisciplinary Digital Publishing Institute.

[41]. Kim, W., Cho, H., Kim, J., Kim, B., and Lee, S. 2020. Target classification using combined yolo-svm in high-resolution automotive fmcw radar. In *2020 ieee radar conference (radarconf20)*, pages 1–5. IEEE.

[42]. Wang, Q. and Xu, S. 2022. Vehicle width detection based on millimeter-wave lfmcw radar for autonomous driving. In *2022 ieee 95th vehicular technology conference:(vtc2022-spring)*, pages 1–6. IEEE.

[43]. Shrestha, A. 2021. Radar based discrete and continuous activity recognition for assisted living. PhD thesis, University of Glasgow.

[44]. Wang, Z., Miao, X., Huang, Z., and Luo, H. 2021. Research of target detection and classification techniques using millimeter-wave radar and vision sensors. *Remote sensing*, 13(6):1064. Multidisciplinary Digital Publishing Institute.

[45]. Komissarov, R. and Wool, A. 2021. Spoofing attacks against vehicular fmcw radar. *Arxiv preprint arxiv:2104.13318*.

[46]. Yang, T. and Lv, C. 2021. A secure sensor fusion framework for connected and automated vehicles under sensor attacks. *Arxiv preprint arxiv:2103.00883*.

[47]. Rodriguez, D., Wang, J., and Li, C. 2021. Spoofing attacks to radar motion sensors with portable rf devices. In *2021 ieee radio and wireless symposium (RWS)*, pages 73–75. IEEE.

[48]. Nashimoto, S., Suzuki, D., Miura, N., Machida, T., Matsuda, K., and Nagata, M. 2021. Low-cost distance-spoofing attack on fmcw radar and its feasibility study on countermeasure. *Journal of cryptographic engineering*, pages 1–10. Springer.

[49]. Moon, T., Park, J., and Kim, S. 2020. Bluefmcw: Random frequency hopping radar for mitigation of interference and spoofing. *Arxiv preprint arxiv:2008.00624*.

[50]. Sun, Z., Balakrishnan, S., Su, L., Bhuyan, A., Wang, P., and Qiao, C. 2021. Who is in control? practical physical layer attack and defense for mmwave-based sensing in autonomous vehicles. *Ieee transactions on information forensics and security*, 16:3199–3214. IEEE.

[51]. Nallabolu, P., Rodriguez, D., and Li, C. 2022. Emulation and malicious attacks to doppler and fmcw radars for human sensing applications. *Ieee transactions on microwave theory and techniques*. IEEE.

[52]. Nallabolu, P. and Li, C. 2021. A frequency-domain spoofing attack on fmcw radars and its mitigation technique based on a hybrid-chirp waveform. *Ieee transactions on microwave theory and techniques*, 69(11):5086–5098. IEEE.

[53]. Lazaro, A., Porcel, A., Lazaro, M., Villarino, R., and Girbau, D. 2022. Spoofing attacks on fmcw radars with low-cost backscatter tags. *Sensors*, 22(6):2145. MDPI.

[54]. Miura, N., Machida, T., Matsuda, K., Nagata, M., Nashimoto, S., and Suzuki, D. 2019. A low-cost replica-based distance-spoofing attack on mmwave fmcw radar. In *Proceedings of the 3rd acm workshop on attacks and solutions in hardware security workshop*, pages 95–100.

[55]. Ordean, M. and Garcia, F. D. 2022. Millimeter-wave automotive radar spoofing. *Arxiv preprint arxiv:2205.06567*.

[56]. Rastogi, N., Rampazzi, S., Clifford, M., Heller, M., Bishop, M., and Levitt, K. 2022. Explaining radar features for detecting spoofing attacks in connected autonomous vehicles. *Arxiv preprint arxiv:2203.00150*.

[57]. Xu, Y., Han, X., Deng, G., Li, G., Liu, Y., Li, J., and Zhang, T. 2022. Sok: Rethinking sensor spoofing attacks against robotic vehicles from a systematic view. *Arxiv preprint arxiv:2205.04662*.

[58]. Shen, J., Wang, N., Wan, Z., Luo, Y., Sato, T., Hu, Z., Zhang, X., Guo, S., Zhong, Z., Li, K., et al. 2022. Sok: On the semantic ai security in autonomous driving. *Arxiv preprint arxiv:2203.05314*.

[59]. Yan, C., Xu, W., and Liu, J. 2016. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *Def con*, 24(8):109.

[60]. Fioranelli, F., Patel, J., Gürbüz, S. Z., Ritchie, M., and Griffiths, H. 2019. Multistatic human micro-doppler classification with degraded/jammed radar data. In *2019 ieee radar conference (radarconf)*, pages 1–6. IEEE.

[61]. Patel, J. S., Fioranelli, F., Ritchie, M., and Griffiths, H. D. 2019. Fusion of deep representations in multistatic radar networks to counteract the presence of synthetic jamming. *Ieee sensors journal*, 19(15):6362–6370. IEEE.

[62]. Damarla, T., Bradley, M., Mehmood, A., and Sabatier, J. M. 2012. Classification of animals and people ultrasonic signatures. *Ieee sensors journal*, 13(5):1464–1472. IEEE.

[63]. Villeval, S., Bilik, I., and Gürbuz, S. Z. 2014. Application of a 24 ghz fmcw automotive radar for urban target classification. In *2014 ieee radar conference*, pages 1237–1240. IEEE.

[64]. ARIK, D. T., KARAL, Ö., and ŞAHİN, A. B. 2013. A comparative study of artificial neural networks and naïve bayes techniques for the classification of radar targets. *Bitlis eren üniversitesi fen bilimleri dergisi*, 9(4):1779–1788.

[65]. Zabalza, J., Clemente, C., Di Caterina, G., Ren, J., Soraghan, J. J., and Marshall, S. 2014. Robust pca micro-doppler classification using svm on embedded systems. *Ieee transactions on aerospace and electronic systems*, 50(3):2304–2310. IEEE.

[66]. Sornin, N., Luis, M., Eirich, T., Kramp, T., and Hersent, O. 2015. Lorawan specification. *Lora alliance*.

[67]. Li, Y., Peng, Z., and Li, C. 2017. Potential active shooter detection using a portable radar sensor with micro-doppler and range-doppler analysis. In *2017 International applied computational electromagnetics society symposium (ACES)*, pages 1–2. IEEE.

[68]. Sasakawa, D., Honma, N., Nakayama, T., and Iizuka, S. 2018. Human identification using mimo array. *Ieee sensors journal*, 18(8):3183–3189. IEEE.

[69]. Zhao, Y.-L., Wang, X.-S., Wang, G.-Y., Liu, Y.-H., and Luo, J. 2007. Tracking technique for radar network in the presence of multi-range-false-target deception jamming. *ACTA electonica sinica*, 35(3):454.

[70]. Fairchild, D. P. and Narayanan, R. M. 2014. Classification of human motions using empirical mode decomposition of human micro-doppler signatures. *Iet radar, sonar & navigation*, 8(5):425–434. IET.

[71]. Sang, Z. and Kang, W. 2020. A fsk radar with frequency-scanned array for moving and stationary human subjects detection. In *Proceedings of the 2020 4th international conference on electronic information technology and computer engineering*, pages 248–252.

[72]. Ilioudis, C. V., Clemente, C., and Soraghan, J. 2019. Understanding the potential of self-protection jamming on board of miniature uavs. In *2019 international radar conference (radar)*, pages 1–6. IEEE.

[73]. Boche, H., Schaefer, R. F., and Poor, H. V. 2020. Denial-of-service attacks on communication systems: Detectability and jammer knowledge. *Ieee transactions on signal processing*, 68:3754–3768. IEEE.

[74]. Tekerek, A. and Yapici, M. M. 2022. A novel malware classification and augmentation model based on convolutional neural network. *Computers & security*, 112:102515. Elsevier.

[75]. Gulatas, I., Kilinc, H. H., Zaim, A. H., and Aydin, M. A. 2023. Malware threat on edge/fog computing environments from internet of things devices perspective. *Ieee access*, 11:33584–33606. IEEE.

[76]. Hur, J. and Nam, H. 2022. Performance comparison of moving target classification based on deep learning. In *2022 13th international conference on information and communication technology convergence (ICTC)*, pages 1533–1535. IEEE.

[77]. Kim, Y. and Moon, T. 2015. Human detection and activity classification based on micro-doppler signatures using deep convolutional neural networks. *Ieee geoscience and remote sensing letters*, 13(1):8–12. IEEE.

İNTİHAL RAPORU İLK SAYFASI

MUHAMMET TALHA BÜYÜKAKKAŞLAR

ORİJİNALLİK RAPORU

%5	%5	%2	%3
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	Submitted to The Scientific & Technological Research Council of Turkey (TUBITAK) Öğrenci Ödevi	%2
2	acikbilim.yok.gov.tr İnternet Kaynağı	%1
3	v1.overleaf.com İnternet Kaynağı	%1
4	toad.halileksi.net İnternet Kaynağı	<%1
5	Holger Boche, Rafael Felix Schaefer, H. Vincent Poor. "Denial-of-Service Attacks on Communication Systems: Detectability and Jammer Knowledge", IEEE Transactions on Signal Processing, 2020 Yayın	<%1
6	strathprints.strath.ac.uk İnternet Kaynağı	<%1
7	Holger Boche, Rafael F. Schaefer, H. Vincent Poor. "On the Algorithmic Solvability of Channel Dependent Classification Problems in	<%1

ETİK KURUL İZİN YAZISI

Uyarı: Canlı denekler üzerinde yapılan tüm araştırmalar için Etik Kurul Belgesi alınması zorunludur.

☐ **Etik Kurul izni gerekmektedir.**

☒ **Etik Kurul izni gerekmemektedir.**

Muhammet Talha BÜYÜKAKKAŞLAR

KURUM İZNİ YAZILARI

Uyarı: Canlı ve cansız deneklerle yapılan tüm çalışmalar için kurum izin belgelerinin eklenmesi zorunludur. Gizlilik ve mahremiyet içeren durumlarda kurum adı kapatılmalıdır.

☐ **Etik Kurul izni gerekmektedir.**

☒ **Etik Kurul izni gerekmemektedir.**

Muhammet Talha BÜYÜKAKKAŞLAR

ÖZGEÇMİŞ