T.C.

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

ELEKTRONİK VE BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

RF PARMAK İZİ KULLANILARAK IoT CİHAZ TANIMADA META AŞIRI ÖĞRENME MAKİNASI TABANLI BAŞARIM ANALİZİ

DOKTORA TEZİ

HÜSEYİN PARMAKSIZ

TEZ DANIŞMANI

PROF. DR. CİHAN KARAKUZU

BİLECİK, 2023

10559728

T.C.

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

ELEKTRONİK VE BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

RF PARMAK İZİ KULLANILARAK IoT CİHAZ TANIMADA META AŞIRI ÖĞRENME MAKİNASI TABANLI BAŞARIM ANALİZİ

DOKTORA TEZİ

HÜSEYİN PARMAKSIZ

TEZ DANIŞMANI

PROF. DR. CİHAN KARAKUZU

BİLECİK, 2023

10559728

BEYAN

RF Parmak İzi Kullanılarak IoT Cihaz Tanımada Meta Aşırı Öğrenme Makinası Tabanlı Başarım Analizi adlı doktora tezi hazırlık ve yazımı sırasında bilimsel ahlak kurallarına uyduğumu, başkalarının eserlerinden yararlandığım bölümlerde bilimsel kurallara uygun olarak atıfta bulunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, tezin herhangi bir kısmının Bilecik Şeyh Edebali Üniversitesi veya başka bir üniversitede başka bir tez çalışması olarak sunulmadığını, aksinin tespit edileceği muhtemel durumlarda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Bu çalışmanın,

Bilimsel Araştırmalar Projeleri (BAP), TÜBİTAK veya benzeri kuruluşlarca desteklenmesi durumunda; projenin ve destekleyen kurumun adı proje numarası ile birlikte beyan edilmelidir.

DESTEK ALINMIŞTIR	**X**	**DESTEK ALINMAMIŞTIR**	

Destek alındı ise;

Destekleyen Kurum: Bilecik Şeyh Edebali Üniversitesi

Desteğin Türü		**Proje Numarası**
1- BAP (Bilimsel Araştırma Projesi)	**Evet**	**2021-01.BŞEÜ.01-01**
2- TÜBİTAK		
Diğer;		

Hüseyin PARMAKSIZ

Tarih

İmza

ÖN SÖZ

Bu çalışmamda yol gösterici yönlendirmeleri ve her konuda destekleri için tez danışmanım Prof. Dr. Cihan KARAKUZU'ya, tez izleme komitesi üyeleri Prof. Dr. Alpaslan DUYSAK ve Dr. Öğr. Üyesi Süleyman UZUN'a ayrıca mühendislik disiplinini ve ahlakını bana aşılayan Prof. Dr. Uğur YÜZGEÇ'e teşekkür ederim. Mesleğimi sevdiren ve her şartta yanımda olan Öğr. Gör. Murat ÖZALP'e sonsuz teşekkür ve saygılarımı sunarım. Her zaman güler yüzü ile elektronik alanında danışabildiğim Doç. Dr. Emrah DOKUR'a teşekkür ediyorum. Ayrıca yazılım tanımlı radyo seçiminde tecrübelerini aktaran Doç. Dr. Muhammet Nuri SEYMAN hocama ve RF alanında özgün bilgilerinden faydalandığım Dr. Öğr. Üyesi Memduh KÖSE hocama içten teşekkürlerimi sunarım.

Üzerimdeki emeklerini hiçbir zaman ödeyemeyeceğim annem ve babama, her konuda desteğini esirgemeyen kıymetli eşim Esra PARMAKSIZ ve sevgili oğlum Alptuğ PARMAKSIZ'a tüm kalbimle teşekkür ederim.

Hüseyin PARMAKSIZ

2023

ÖZET

RF PARMAK İZİ KULLANILARAK IoT CİHAZ TANIMADA META AŞIRI ÖĞRENME MAKİNASI TABANLI BAŞARIM ANALİZİ

Günümüzün gözde teknolojilerinden biri olan IoT kavramının ortaya çıkması, akıllı cihazların getirdiği kolaylıklar ve kullanımının yaygınlaşmasıyla birlikte kablosuz cihazların sayısı artmakta ve buna bağlı olarak cihazlar arasında yoğun ve karmaşık bilgi iletişim ağları oluşmaktadır. IoT uygulamalarında yaygın olarak kullanılan birçok cihaz türü, farklı iletişim standartlarını kullanarak haberleşmektedir. Haberleşme sürecinde bilgi iletişim ağlarına yetkisiz erişim ve saldırıları önlemek amacıyla güvenlik kavramı ön plana çıkmaktadır. Fakat, IoT cihazlarının doğası gereği kaynakları kısıtlıdır. Bu nedenle, cihazlarda güvenlikle ilgili özelleştirilmiş önlemlerin alınması mümkün olmamaktadır. Güvenlik sorununu çözmek için cihazların donanımsal tekilliğini barındıran RF parmak izleri IoT cihazlarını tanımlamak ve doğrulamak için kullanılmaktadır. Bu çalışmada, düşük maliyetli yazılım tanımlı radyo, tek kartlı bir bilgisayar ve açık kaynaklı yazılım kullanarak tasarlanmış ve gerçeklenmiş bir sistem ile RF sinyalleri yakalanıp kayıt altına alınmıştır. Yakalanan sinyallerin özniteliklerini çıkarmak için sinyalin geçici bölgesi/kısmı belirlenir ve Hilbert dönüşümü (HD) kullanılarak anlık genlik (AG), anlık faz (AFa) ve anlık frekans (AFr) değerleri elde edilmiştir. En baskın öznitelikleri seçmek için bu değerlere çarpıklık, basıklık, standart sapma, varyans ve medyan değer gibi çeşitli istatistiksel yöntemler uygulanmamıştır. Öznitelik boyutu, minimum artıklık ve maksimum alaka düzeyi tekniği kullanılarak indirgenmiştir. IoT cihazı tanımlama için sınıflandırıcı olarak AÖM tabanlı Meta-AÖM, Çok Katmanlı Meta-AÖM (ÇK-Meta-AÖM) ve Kısıtlı Karma Meta-AÖM (KK-Meta-AÖM) ağ yapıları ve bu yapılar için AÖM tabanlı öğrenme algoritmaları kullanılmıştır. Anılan son iki AÖM tabanlı ağ yapısı bu tez çalışması kapsamında geliştirilmiş özgün ağ yapılarıdır. Bu sınıflandırıcıların başarımı, 7 cihazdan alınan 3752 ham sinyalden oluşan özgün veri kümesine göre deneysel olarak değerlendirilmiştir. Deneysel değerlendirmeler sonucunda, ÇK-Meta-AÖM ağının cihazları %88 doğruluk oranıyla, Meta-AÖM ağının ise %90 civarında bir doğruluk oranıyla cihazları ayırt ettiği gözlenmiştir. KK-Meta-AÖM ağının ise, %92'lik bir doğruluk oranıyla en iyi başarım gösterdiği sonucuna varılmıştır.

Anahtar Kelimeler: Meta aşırı öğrenme makinası, IoT güvenliği, RF parmak izi, SDR.

ABSTRACT

META EXTREME LEARNING MACHINE BASED PERFORMANCE ANALYSIS FOR IoT DEVICE IDENTIFICATION USING RF FINGERPRINT

The IoT revolution has led to exponential growth in wireless devices, creating intricate communication networks. Ensuring the security of these networks is crucial to prevent unauthorized access and attacks. However, IoT devices have limited resources, making it challenging to implement customized security measures. To address this, RF fingerprints, which capture the unique hardware characteristics of devices, are used for identification and authentication. In this study, a system was developed using cost-effective software-defined radio (SDR), a single-board computer, and open-source software to capture and record RF signals. Features of the signals were extracted by identifying the transient region and applying the Hilbert Transform to obtain Instantaneous Amplitude, Instantaneous Phase, and Instantaneous Frequency values. Rather than traditional statistical methods, the feature dimension was reduced using the Minimum Redundancy Maximum Relevance (MRMR) technique. For IoT device identification, classifiers such as ELM-based Meta-ELM, Multilayer Meta-ELM (ML-Meta-ELM), and Constrained Mixed Meta-ELM (CM-Meta-ELM) network structures were used, along with ELM-based learning algorithms. The ML-Meta-ELM network achieved an 88% accuracy in distinguishing devices, while the Meta-ELM network achieved around 90%. The CM-Meta-ELM network demonstrated the highest performance with a 92% accuracy rate.

Keywords: Meta Extreme Learning Machine, IoT security, RF fingerprinting, SDR.

İÇİNDEKİLER

Sayfa

TABLOLAR LİSTESİ

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

KISALTMALAR VE SİMGELER LİSTESİ

ADC	**:**	Analog to Digital Converter (Analog Dijital Dönüştürücü)
ADS-B	**:**	Automatic Dependent Surveillance-Broadcast (Otomatik Bağımlı Gözetim-Yayın)
AE	**:**	Auto Encoding (Otomatik Kodlayıcı)
AFa	**:**	Instantaneous Phase (Anlık Faz)
AFH	**:**	Adaptive Frequency Hopping (Uyarlanabilir Frekans Atlama)
AFr	**:**	Instantaneous Frequency (Anlık Frekans)
AG	**:**	Instantaneous Amplitude (Anlık Genlik)
AI	**:**	Artificial Intelligence (Yapay Zekâ)
AÖM	**:**	Aşırı Öğrenme Makinasi (Extreme Learning Machine)
BRCD	**:**	Bayesian Ramp Change Detection (Bayesian Ramp Değişikliği Tespiti)
BSCD	**:**	Bayesian Step Change Detection (Bayesian Adım Değişikliği Tespiti)
BVK	**:**	Tez Kapsamında Oluşturulan Özgün Veri Kümesi
CCK	**:**	Complementary Code Keying (Tamamlayıcı Kod Anahtarlama)
ÇK-AÖM	**:**	Çok Katmanlı Aşırı Öğrenme Makinası (Multi Layer Extreme Learning Machine)
ÇK-Meta-AÖM	**:**	Çok Katmanlı Meta Aşırı Öğrenme Makinası (Multi Layer Meta Extreme Learning Machine)
DAC	**:**	Digital to Analog Converter (Dijital Analog Dönüştürücü)
dB	**:**	Decibel (Desibel)
DHSS	**:**	Direct Sequence Spread Spectrum (Doğrudan Dizili Yayılı Spektrum)
FHSS	**:**	Frequency Hopping Spread Spectrum (Frekans Atlamalı Yayılı Spektrum)
FPGA	**:**	Field Programmable Gate Array (Alan Programlanabilir Kapı Dizileri)
GHz	**:**	Gigahertz (Bir milyar hertz)
GLRTD	**:**	Generalized Likelihood Ratio Test Detection (Genelleştirilmiş İhtimal Oranı Testi Tespiti)
GNR	**:**	GNU Radio (GNU Radyo)
GSM	**:**	Mobil iletişim için küresel sistem (Global System for Mobile Communications)

IEEE	**:**	Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
IF	**:**	Intermediate Frequency (Orta düzey frekans)
IoT	**:**	Internet of Things (Nesnelerin İnterneti)
ISM	**:**	Industrial, Scientific and Medical (Endüstriyel, Bilimsel ve Tıbbi)
ITS	**:**	Information Theoretic Security (Bilgi Teorik Güvenlik)
JOA-VK	**:**	Justice Owusu Agyemang'ın Veri Kümesi
K-AÖM	**:**	Kısıtlı Aşırı Öğrenme Makinası (Constrained Extreme Learning Machine)
KK-Meta-AÖM	**:**	Kısıtlı Karma Meta Aşırı Öğrenme Makinası (Constrained Mixed Meta Extreme Learning Machine)
LOS	**:**	Line-of-sight (Doğrusal görüş hattı)
LTE	**:**	Long-Term Evolution (Uzun dönemli gelişim)
MCPD	**:**	Mean Change Point Detection (Ortalama Değişim Noktası Tespiti)
MEC	**:**	Mobile Edge Computing (Mobil Kenar Hesaplama)
M2M	**:**	Machine to Machine (Makineden makineye)
Meta-AÖM	**:**	Meta Aşırı Öğrenme Makinası (Meta Extreme Learning Machine)
MHz	**:**	Megahertz (Bir milyon hertz)
MIMO	**:**	Multiple-Input Multiple-Output (Çoklu Giriş Çoklu Çıkış)
ML	**:**	Machine Learning (Makina Öğrenmesi)
MRMR	**:**	Maximum Relevance Minimum Redundancy (Maksimum İlgi Minimum Gereksizlik)
NLOS	**:**	Non-line-of-sight (Doğrusal görüş dışı/görüş hattı dışı)
OS	**:**	Operating System (İşletim Sistemi)
PCA	**:**	Principal Component Analysis (Temel Bileşen Analizi)
PD	**:**	Phase Detection (Faz Tespiti)
PE	**:**	Permutation Entropy (Permütasyon Entropisi)
PER	**:**	Packet Error Rate (Paket Hata Oranı)
PHY	**:**	Physical Layer (Fiziksel Katman)
PN	**:**	Pseudo-noise (Rastgele gürültü)
QoS	**:**	Quality of Service (Hizmet Kalitesi)
RF	**:**	Radio Frequency (Radyo Frekansı)

RPi	**:**	Raspberry Pi
RSSI	**:**	Received Signal Strength Indicator (Alınan Sinyal Gücü Göstergesi)
SaaS	**:**	Software as a Service (Hizmet Olarak Yazılım)
SDN	**:**	Software Defined Network (Yazılım Tanımlı Ağ)
SDR	**:**	Software Defined Radio (Yazılım Tanımlı Radyo)
SEC	**:**	Superiority of Energy Criterion (Enerji Kriterinin Üstünlüğü)
SLFN	**:**	Single hidden layer feed forward neural network (Tek Gizli Katmanlı İleri Beslemeli Sinir Ağı)
SNR	**:**	Signal to Noise Ratio (Sinyal Gürültü Oranı)
SRC	**:**	Sample Rate Conversion (Örnek Oran Dönüşümü)
TCP/IP	**:**	Transmission Control Protocol/InternetProtocol (İletim Denetimi Protokolü / Internet Protokolü)
USB	**:**	Universal Serial Bus (Evrensel Seri Veri yolu)
USRP	**:**	Universal Software Radio Peripheral (Evrensel Yazılım Radyo Çevre Birimi)
VFDTD	**:**	Variance Fractal Dimension Threshold Detection (Varyans Fraktal Boyut Eşik Tespiti)
VNC	**:**	Virtual Network Computing (Sanal Ağ İletişim Protokolü)
Wi-Fi	**:**	Wireless Fidelity (Kablosuz Bağlantı)
WSN	**:**	Wireless Sensor Networks (Kablosuz Sensör Ağları)
YSA	**:**	Yapay Sinir Ağları (Artificial Neural Networks)

1. GİRİŞ

Teknolojinin gelişmesi ve getirdiği kolaylıklar ile IoT kullanımı hızla artmaktadır. IoT, kablosuz özelliği olan akıllı cihazlar ile internet arasında veri aktarımı sağlayan bir köprü görevini üstlenmektedir. Akıllı cihazların sayısındaki artışla birlikte, cihaz iletişimini gerçekleştirmek için kablosuz teknolojiyi kullanmasına izin verecek bol ve karmaşık bir bilgi ağı oluşmaktadır. İnternet sadece insanları birbirine bağlamakla kalmayıp, aynı zamanda insanları ve nesneleri, nesneleri ve nesneleri de birbirine bağlamaktadır. Son yıllarda, MEC ile geleneksel IoT mimarisini birleştiren yenilikçi bir IoT değerler dizisi ortaya koyulmaktadır (S. Chen vd., 2019). MEC, IoT cihazları arasında, endüstriyel denetim uygulamaları için kritik konular olan çevik bağlantı, gerçek zamanlı hizmetler, veri optimizasyonu, uygulama zekâsı, güvenlik ve gizlilik koruması açısından endüstriyel sayısallaşmanın kritik ihtiyaçlarını karşılamak için uç akıllı hizmetler sağlayan uzak bulut cihazları için bir köprü görevi görmektedir (Zhang, Leng, He, Maharjan, & Zhang, 2018). Bu büyük ağda bilgi koruma ve güvenliğinin önemi göz ardı edilemez. Geleneksel kimlik doğrulama bilgileri, ağ içinde güvenli veri iletişimini gerçekleştiren simetrik şifreleme dediğimiz şekliyle, alıcının anahtarı doğrulamasını sağlayan bir mesaj kimlik doğrulama kodu ve anahtarı gibi bilgileri doğrulamak için sıklıkla tanımlayıcılarla işaretlenmektedir (Muhal, Luo, Mahmood, & Ullah, 2018). IoT gibi büyük ve karmaşık bir ağ karşısında tüm düğümlerin aynı anahtarı paylaşması sakıncalı ve riskli olmaktadır. Bilgi güvenliğinin yetersiz olduğu durumlarda, IoT cihazlarının donanım kısıtlamaları ile uyumlu yeni bir teknolojik güvenlik çözümünün geliştirilmesi gerekmektedir. Bu bağlamda, cihazların donanımsal özelliklerinin sağladığı tekilliği sergileyen RF parmak izi teknolojisi çözüm sunması bu tez çalışmasının ana omurgasını oluşturmaktadır.

RF parmak izi, bir dinleyicinin sesin doğal varyasyonlarına ve özelliklerine dayalı olarak bir konuşmacıyı nasıl tanımlayabileceğine benzer şekilde çalışmaktadır. Bir işlem sırasında sinyalin zaman alanı ve frekans alanı özelliklerini çıkararak, bir RF parmak izi, alandaki farklı kablosuz cihazları otomatik olarak tanımlayabilmektedir (Lin, Lai, & Chen, 2020). Cihazlar, üretim aşamasında tekrarlanamazlığı destekleyen kontrol edilemeyen rastgele fiziksel değişikliklere, rastgeleliğe ve benzersizliğe sahip olabilmektedir. Literatürde bu özellikler RF parmak izi olarak adlandırılmaktadır. RF parmak izi, ayrı bir fiziksel güvenlik katmanı olarak kullanılabilir. Ek olarak, güvenliği artırmak için OSI modelinin diğer katmanlarıyla çok faktörlü kimlik doğrulama için değerlendirilebilir (Lin vd., 2020).

Cihazların RF parmak izi özelliklerini sayısal olarak işlemek ve analiz etmek için bir donanım ve yazılım birlikteliği gerekmektedir. Ayrı donanım ve yazılım bileşenlerinin kullanılmasını önlemek için SDR'ler kullanılmaktadır. Literatürde SDR'ler radyo iletişimi için kullanılmaktadır. SDR, donanım tabanlı çözümlerin aksine radyo ve kablosuz iletişim protokollerini temel alan bir teknolojidir. Yeniden programlanabilme özelliği sayesinde ek bir donanım gerektirmeksizin ihtiyaçları karşılamaktadır. Bu sayede çok işlevli ve çok bantlı radyo ve kablosuz cihazlarda çalışma imkanı sağlamaktadır (Akeela & Dezfouli, 2018). SDR, geleneksel donanım iletişim cihazı uygulamasının yerini alan, yeniden yapılandırılabilir bir kablosuz iletişim sistemi oluşturan önemli bir teknolojik gelişmedir. Küçük tasarım değişiklikleri için sıfırdan donanım kurmak veya mevcut bir sisteme yeni donanım eklemek zor ve pahalı olmaktadır. SDR, aynı donanım platformunun farklı protokollere sahip birden çok iletişim ekipmanı için yeniden kullanılmasını sağlayarak son kullanıcı için hizmet süresini ve geliştirme maliyetlerini azaltır (Sruthi, Abirami, Manikkoth, Gandhiraj, & Soman, 2013). SDR'ler fiziksel olarak küçük boyutları ve düşük güç tüketimleri nedeniyle (Paillassa & Morlet, 2003), araçtan araca (V2V) iletişim sistemlerinin (Xiang, Sotiropoulos, & Liu, 2015), küresel navigasyon uydu sistemi (GNSS) sensörleri (Seo vd., 2011) ve IoT uygulamaları (Y. Chen vd., 2016), (Y. Park vd., 2016) gibi sistemlerin tasarımı ve uygulanması için uygundur.

SDR cihazlarıyla kaydedilen RF ham sinyalinin geçici, giriş ve sabit durum bölümleri dahil olmak üzere farklı kısımlarını kullanarak RF parmak izi özniteliklerini belirlemek için çeşitli teknikler kullanılır. Bu teknikler, Hızlı Fourier Dönüşümü (FFT), Zaman-Frekans Analizi, Döngüsel Durağan Analiz, Makina Öğrenimi ve diğerlerini içerir. Wi-Fi RF sinyalleri genellikle frekans modülasyonu (FM) veya faz kaydırma anahtarlı (PSK) modülasyon teknikleri ile taşınır. Sinyalde bulunan frekans bileşenlerinin dağılımı, darbe genişliğini ve modülasyon tayfını tanımlar. Bu özellikleri belirlemek için HD yöntemi kullanılır. Ayrıca bu öznitelikler, sınıflandırma algoritmalarında sinyal kaynağının tanımlanması için veri kümeleri oluşturur.

Son on yılda, birçok sinir ağı mimarisi geliştirilmiştir. İleri beslemeli sinir ağları en çok çalışılanlar arasındadır. Polinom olmayan aktivasyon fonksiyonlarına sahip çok katmanlı bir ileri beslemeli sinir ağının, herhangi bir sürekli fonksiyona yaklaşma yeteneğine sahip olduğu gösterilmiştir. Araştırmacılar, model basitliği ve nispeten yüksek öğrenme ve yanıt verme hızları nedeniyle SLFN'leri kapsamlı bir şekilde incelemiş ve kullanmışlardır. Yakın geçmişte, Huang ve ark. (G.-B. Huang, Zhu, & Siew, 2006), SLFN'lerin son derece hızlı öğrenen yeni bir

modeli olan AÖM öğrenme kavramını tanımlamışlardır. AÖM, sınıflandırma, regresyon ve yarı denetimli, denetimli ve denetimsiz görevler için birleşik bir çerçeve sağlamaktadır (G.-B. Huang, Zhou, Ding, & Zhang, 2011; G. Huang, Song, Gupta, & Wu, 2014; Karakuzu, 2019). Bu avantajlar, AÖM'yi hem araştırmacılar hem de mühendisler arasında popüler kılmaktadır (W. Zhu, Miao, & Qing, 2015).

ÇK-AÖM ilk olarak 2006'da önerilmiştir (G.-B. Huang, Zhu, vd.., 2006). Araştırmacılar, AÖM algoritmasını çok katmanlı ağlara uyarlayarak ÇK-AÖM algoritmasını geliştirdiler. Bu ilave katmanlar sayesinde, daha karmaşık sınıflandırma problemlerini çözmek için daha fazla öznitelik çıkarabilir. Hızlı öğrenme ve yüksek doğruluk oranları sağlayan birçok uygulamada da kullanılır. (W. Zhu vd., 2015), geleneksel bir AÖM ağ yapısında gizli düğümlerin girdi ağırlıklarını atamak için örnek vektörlerin basit bir doğrusal kombinasyonunu kullanma fikriyle kısıtlı aşırı öğrenme makinaları (CELM'leri) tanıtmıştır. Örnek dağılımına dayalı olarak gizli nöronların parametrelerini rastgele seçmek için CELM'ler adı verilen yeni atama yöntemleri önerdiler. Gizli düğümlerin giriş bağlantı ağırlıklarını rastgele seçen AÖM'nin aksine, CELM'ler gizli düğümlerin bu parametrelerini gerçek örnek vektörlerin bazı temel birleştirmelerini içeren kısıtlanmış bir vektör uzayından rastgele seçerler.

Bu çalışmada IoT cihazlarının RF parmak izi sinyallerinden tanımlanması için bu alanda ilk kez AÖM gruplarına dayalı algoritmalar kullanılmıştır. Bu ağların RF parmak izinden IoT cihazının tanımlanmasında kullanımı analiz edilmiştir. Meta-AÖM ve CELM'lerden Constrained Mixed (kısıtlı karma) AÖM'ün başlangıç ağırlık ve bias atama işlemlerini birleştirerek KK-Meta-AÖM adını verdiğimiz ve Meta-AÖM'nin temel AÖM'si olarak ÇK-AÖM'yi kullanma fikri ile tasarladığımız ve ÇK-Meta-AÖM olarak adlandırdığımız iki yeni AÖM ağı tanımlanmıştır.

Ayrıca çalışmada 2.4 GHz frekans bandında kablosuz olarak haberleşen IoT cihazlarının güvenliği için RF parmak izi veri toplama sistemi tasarlanmıştır. Tasarımda açık kaynaklı yazılımlar ve düşük maliyetli SDR kullanılmıştır. Sinyal yakalama ve işleme süreçlerinde HackRF One SDR, RPi-4, DragonOS_Pi64, shell scripts, iperf3 ve GNU Radio (GNR) programı ile gerçeklenmiş veri toplama sistemi kullanılmıştır.

Özellik çıkarma işleminde sinyalin geçici bölgesi/bölümü belirlendikten sonra HD ve istatistiksel yöntemler (çarpıklık, basıklık, varyans, medyan vd.) kullanılmıştır. MRMR, özellik seçimi ve indirgeme için kullanılmıştır. Meta-AÖM, KK-Meta-AÖM ve ÇK-Meta-AÖM

algoritmalarının RF parmak izi tanıma sistemlerinde sınıflandırıcı olarak başarımları değerlendirilmiştir. Daha önce de bahsedildiği gibi bu türden sınıflayıcıların kullanılması bu alanda bir ilktir ve literatüre bu bağlamda yenilik sağlamıştır.

1.1. Literatür Araştırması

IoT cihazlardan RF parmak izi elde etmek için yaygın olarak Wi-Fi, Bluetooth, GSM, LTE ve ADS-B bileşenleri kullanılmaktadır. Wi-Fi bileşenleri, geniş mesafelerde (genellikle 100 metre veya daha fazla) veri transferi için kullanılmaktadır. Bluetooth bileşenleri, kısa mesafelerde (genellikle 10 metre veya daha az) veri transferi için kullanılmaktadır. Bluetooth cihazlarının RF parmak izi, cihazın özellikleri, anten yapısı ve çevresindeki nesneler gibi fiziksel özellikler göz önünde bulundurularak elde edilebilmektedir. GSM bileşenleri ise, 2G, 3G ve 4G gibi mobil veri transferi için kullanılmaktadır.

Wi-Fi cihazları genellikle 2.4 GHz ve 5 GHz aralığında frekanslarda yayın yaparlar. Bluetooth cihazları genellikle 2.4 GHz frekansında yayın yaparlar. GSM cihazları genellikle 850 MHz veya 900 MHz frekanslarında veri ve sesli çağrı için yayın yapabilirler. GSM, dünya çapında yaygın olarak kullanılan bir mobil telefon standardıdır ve 900 MHz veya 1.8 GHz frekans bandında çalışmaktadır.

RF parmak izi elde etmek için *Spektrogram analizi*, *demodülasyon*, *çoklu anten* sistemleri v.b. tekniklerden faydanılmaktadır. Wi-Fi, GSM ve Bluetooth cihazlarının RF parmak izi, cihazın özellikleri, anten yapısı, cihazın kullanımı ve çevresindeki nesneler gibi fiziksel özellikler göz önünde bulundurularak elde edilmektedir. IoT cihazlarının çoğunluğunda yaygın olarak kullanılan haberleşme protokolü Wi-Fi olduğundan tezde tercih sebebi olmuştur. Ayrıca 2022 yılında *Wi-Fi 6E* standardı kabul edilmiş ve cihazlar üzerindeki uygulamaları artmıştır. Bu yeni standardın tanıttığı 6 GHz frekans bandı, daha geniş kanal aralıkları ve daha yüksek bant genişliği sunarak Wi-Fi cihazlarının daha iyi tanımlanmasına olanak sağlamaktadır. Kablosuz - MIMO teknolojisi, Wi-Fi cihazları arasında aynı anda birden fazla veri akışını desteklemektedir. Bu teknoloji, cihazların benzersiz veri alışverişi davranışlarını kullanarak cihaz tanımlama için kullanılabilmektedir. Wi-Fi cihaz tanımlama alanında makina öğrenimi ve yapay zeka tekniklerinin kullanımı önemli bir ilerleme kaydetmiştir. Bu teknikler, cihazların davranış modellerini analiz ederek onları tanımlamak için kullanılmaktadır. Wi-Fi cihazlarının sinyal özelliklerinin analizi onları tanımlamak için önemli bir yöntemdir. 2022-2023 arasında, *sinyal işleme ve spektral analiz teknikleri* üzerine yapılan çalışmalar Wi-Fi cihaz

tanımlama başarımını artırmıştır. Wi-Fi *cihaz tanımlama, güvenlik ve gizlilik* konularını da beraberinde getirmektedir.

IEEE ICSPCC 2013 konferansında *"Detection of Wi-Fi transmitter transients using statistical method"* başlıklı bildiride, Wi-Fi verileri üzerinden parmak izi tanımlamasında geçici durum tespitinin önemli olduğu vurgulanmaktadır. Geleneksel yöntemlerin (Varyans Fraktal Boyut Eşik Tespiti, Bayes Adım Değişimi Tespiti ve Faz Tespiti) ihtiyaç duyduğu karmaşıklık, doğruluk ve eşik gibi dezavantajlara göre, bu çalışmada istatistiksel yönteme dayalı geliştirilmiş bir algoritma (Ortalama Değişim Noktası Tespitine dayalı) ortaya konulmaktadır ve yalnızca maksimum istatistiksel farkın konumunu hesaplayarak geçici durumu tespit etmektedir (L. Huang vd., 2013).

IEEE Symposium on CISDA sempozyumunda *"Framework for automatic signal classification techniques (FACT) for software defined radios"* başlıklı bildiride, aynı anda birden fazla sinyali sınıflandırabilen yazılım tanımlı radyolar (SDR) ile otomatik sinyal sınıflandırma teknikleri (FACT) için yeni bir çerçeve tasarlanmış ve sunulmuştur. Bu çalışmanın odak noktası, yeni sınıflandırma yöntemlerinin test edilmesini ve uygulanmasını kolaylaştırmak için modüler bir sınıflandırma çerçevesi oluşturmaktır (J. Jagannath vd., 2015).

Future Computing and Informatics Journal dergisindeki *"A survey of IoT cloud platforms"* başlıklı makale, mevcut IoT bulut hizmeti sağlayıcıları ile bunların artıları ve eksileri hakkında somut biçimde ayrıntılı bilgi sağlamaktadır (Ray, 2016).

IEEE Communications Magazine dergisinde yayınlanan *"EdgeIoT: Mobile Edge Computing for the Internet of Things"* başlıklı makalede, geleneksel nesnelerin interneti mimarisinin ölçeklenebilirlik sorunu ile başa çıkmak adına EdgeIoT mimarisi önerilmektedir (Sun ve Ansari, 2016).

Rajshahi University Journal of Science and Engineering'de *"A practical approach to spectrum analyzing unit using rtl-sdr"* başlıklı makalede, mevcut donanım spektrum analizörünün bir alternatifi olarak ustaca kullanılabilecek bir RTL-SDR tabanlı spektrum analizörü verilmektedir (M. H. Rahman ve Islam, 2016).

IEEE International Symposium on DySPAN sempozyumunda sunulan *"Modulation recognition with GNU radio, keras, and HackRF"* başlıklı bildiri, canlı yayın sinyallerinin

modülasyon türlerini sınıflandırmaya yönelik yaklaşımları üç veri türü kümesi üzerinden bir dizi sinir ağını eğitmek için yazılım tanımlı radyo ile iki basit ve ucuz alıcı-vericinin kullanılmasını içermektedir (Ziegler vd., 2017).

IEEE Journal of Selected Topics in Signal Processing dergisinde *"Over-the-air deep learning based radio signal classification"* başlıklı makale, radyo iletişim sinyalleri için derin öğrenme tabanlı radyo sinyali sınıflandırmasının başarımını değerlendirmektedir (O'Shea vd., 2018).

IEEE Internet of Things Journal'da *"RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning"* başlıklı makalede, alıcı ucunda yerinde makina öğrenimi yoluyla tespit edilen, kablosuz vericilerin RF özellikleri üzerindeki doğal süreç değişiminin etkilerini kullanarak, kablosuz düğümlerin gerçek zamanlı kimlik doğrulamasına izin veren derin sinir ağı tabanlı bir çerçeve olan RF-PUF sunulmaktadır (Chatterjee vd., 2018).

IEEE Communications Magazine'de *"Deep learning convolutional neural networks for radio identification"* başlıklı makalede, SDR algılama yeteneği ve makina öğrenimi (ML) tekniklerinin bir kombinasyonunu kullanarak nominal olarak benzer cihazlar arasında belirli bir radyoyu benzersiz şekilde tanımlamak için bir yöntem açıklanmaktadır (Riyaz vd., 2018).

IEEE Journal of Selected Topics in Signal Processing dergisindeki *"Deep Learning for RF Device Fingerprinting in Cognitive Communication Networks"* başlıklı makale, bilişsel radyo cihazlarının fiziksel katman özelliklerinin tespiti için bir dizi IEEE 802.15.4 cihazı ile derin öğrenme çalışmalarını içermektedir. Zaman alanlı karmaşık temel bant hata sinyalini kullanarak evrişimli bir sinir ağını eğitmek için bir çerçeve geliştirilmiştir (Merchant vd., 2018).

arXiv'deki *"Authenticaion of Everything in the Internet of Things: Learning and Enviromental Efects"* başlıklı makalede, farklı IoT cihazlar için farklı çevresel koşullar altında sınıflandırma performansının artırılması için transfer öğrenme yaklaşımı önerilmektedir (Sharaf Dabbagh ve Saad, 2018).

IEEE Transactions on Cognitive Communications and Networking konferansında *"Deep learning models for wireless signal classification with distributed low-cost spectrum sensors"* başlıklı bildiride, dağıtılmış bir kablosuz spektrum algılama ağında modülasyon

sınıflandırma problemi için uzun kısa süreli belleğe (LSTM) dayalı otomatik modülasyon sınıflandırması için yeni bir veri güdümlü model önerilmektedir (Rajendran vd., 2018).

IEEE Access dergisindeki *"Rssi-based indoor localization with the internet of things"* başlıklı makalede iç mekân lokalizasyonu için dört kablosuz teknoloji; Wi-Fi (2,4 GHz bandında IEEE 802.11n-2009), Bluetooth düşük enerji, Zigbee ve uzun menzilli geniş alan ağı karşılaştırılmaktadır (Sadowski ve Spachos, 2018).

IEEE International Conference on EExPolytech konferansında *"Possibility of Peak-toAvegare Power Ratio Reduction by Application of Optimal Signal for Transmitter Based on SDR HackRF One"* başlıklı bildiride, yüksek spektral verimlilik sağlayan en uygun sinyaller için verici HackRF One seçilerek, iletilen dizinin tepe/ortalama güç oranının (PAPR) hem dikdörtgen zarf biçimine sahip klasik sinyaller hem de en uygun olanlar (tepe/ortalama güç oranı kısıtlaması olan ve olmayan) durumunda teorikten daha yüksek olduğu gösterilmektedir (Ishkaev vd., 2018).

Electronics Letters dergisinde *"Deep Learning Based RF Fingerprinting for Device Identification an Wireless Security"* başlıklı makalede derin sinir ağları kullanılarak RF parmak izi çözümü sunulmaktadır. Donanıma özgü özellikleri otomatik olarak tanımlamak ve vericileri sınıflandırmak için LSTM ağı önerilmektedir (Wu vd., 2018).

IEEE MILCOM konferansında sunulan *"IoT Devices Fingerprinting using Deep Learning"* başlıklı bildiride, derin öğrenme algoritmalarından derin sinir ağları, evrişimsel sinir ağları ve tekrarlayan sinir ağları yöntemleriyle kablosuz cihazların sınıflandırma başarımlarının kıyaslaması yapılmaktadır (Jafari vd., 2018).

EURASIP Journal on Wireless Communications and Networking dergisinde sunulan *"Physical layer identification of LoRa devices using constellation trace figure"* başlıklı makalede, LoRa cihazları için fiziksel katman parmak izine dayalı bir tanımlama yöntemi önerilmektedir. Önceki çalışmaların aksine, LoRa cihazlarının radyo frekansı (RF) parmak izi özelliklerinden, özellik eşleştirmeyi görüntü tanımaya dönüştüren bir diferansiyel takımyıldız iz figürü oluşturulmuştur. Diferansiyel takımyıldız iz figürünü analiz etmek için LoRa sinyalinin kümeleme merkezinin Öklid mesafesine dayalı bir sınıflandırma yöntemi uygulanmaktadır (Jiang vd., 2019).

4. Uluslararası FMEC konferansında sunulan *"Intrusion Detection for IoT Devices based on RF Fingerprinting using Deep Learning"* başlıklı çalışma, yetkisiz IoT cihazlarını derin öğrenme kullanarak tespit etmek için yeni bir saldırı tespit yöntemi önermektedir. Önerilen yöntem, fiziksel katman tabanlı özellikler cihaza özgü olduğundan ve taklit edilmesi daha zor olduğundan, RF parmak izine dayanmaktadır. RF izleri, USRP tabanlı bir test yatağı aracılığıyla altı "özdeş" ZigBee cihazından toplanır. İzler, modelin sağlamlığını sağlamak için bir Sinyal-Gürültü Oranı aralığını kapsar. RF izlerinden öznitelikleri çıkarmak için evrişimli bir sinir ağı kullanılır ve çıkarılan öznitelikler üzerinde boyut küçültme ve korelasyon giderme gerçekleştirilir. İndirgenmiş özellikler daha sonra IoT cihazlarını tanımlamak için kümelenir (Bassey vd., 2019).

The Journal of Supercomputing'deki *"The individual identification method of wireless device based on dimensionality reduction and machine learning"* başlıklı makalede, kimlik doğrulama güvenlik sorunlarını çözmek için izinsiz giriş tespitinin bir bileşeni olarak boyutsal küçültme ve makina öğrenmesine dayalı bir RF parmak-izi tanımlama yöntemi önerilmektedir (Y. Lin vd., 2019).

2019 ASET konferansında *"IoT devices security using RF fingerprinting"* başlıklı bildiride, IoT cihazlarından yayılan kablosuz sinyalleri algılamayı amaçlayan evrensel bir SDR (yazılım tanımlı radyo) tabanlı düşük maliyetli uygulama önerilmektedir. Her bir cihazı tanımlamak ve doğrulamak için, ham sinyal yakalama yöntemleri ile bu sinyallerden istatistiksel özelliklerin çıkarılmasına değinilmektedir (Nouichi vd., 2019).

IEEE Wireless Communications dergisindeki *"Physical Layer Security for the IoT: Authentication and Key Generation"* başlıklı makalede, katmana uygulanan RF parmak izi yönteminin IoT güvenliğini sağlamak için nasıl bütünleştirileceği anlatılmaktadır (Junqing Zhang vd., 2019).

IEEE CCECE konferansında sunulan *"Deep Learning: Edge-Cloud Data Analytics for IoT"* başlıklı bildiride, IoT veri analizi için bulut ve uç bilgi işlemin birleştirilmesi araştırılmaktadır. Bulutta makina öğrenmesi, uçta veri azaltmak için otokodlayıcı (autoencoder) derin öğrenme tabanlı yaklaşımlar sunulmaktadır (Ghosh ve Grolinger, 2019).

International Conference on WiMob konferansında sunulan *"Radio Frequency Fingerprint Identification Based on Denoising Autoencoders"* başlıklı bildiride, derin öğrenme

ile RF parmak izi teknikleri için genel bir "Denoizing AutoEncoder (DAE)" adlı model önerilmektedir (J. Yu vd., 2019).

Sensors dergisinde *"Radio Frequency FingerprintBased Intelligent Mobile Edge Computing for IoT Authentication"* başlıklıklı makalede, şifreleme tabanlı yöntemlere dayanmadan mobil kenar bilgi işlem (MEC) senaryosu altında çok sayıda kaynak kısıtlı terminal için kimlik doğrulaması gerçekleştirmek üzere iki katmanlı bir modelle birleşen hafif bir radyo frekansı parmak izi tanıma şeması (RFFID) önerilmektedir. İlk katmanda, MEC cihazları tarafından sinyal toplama, RF parmak izi özelliklerinin çıkarılması, dinamik özellik veritabanı depolama ve erişim kimlik doğrulama kararı gerçekleştirilir. İkinci katmanda, öğrenme özellikleri, karar modelleri oluşturma ve tanıma için makina öğrenimi algoritmalarını uygulama uzak bulut tarafından gerçekleştirilir. Bu sayede, makina öğrenimi eğitim yöntemlerinden ve bulutun bilgi işlem kaynak desteğinden yararlanılarak kimlik doğrulama oranı iyileştirilebilmektedir (S. Chen vd., 2019).

SSRN'de *"Men-in-the-middle attack simulation on low energy wireless devices using software define radio"* başlıklı çalışmada, SDR'lerin karşılaştırmalı bir analizi verilmiş olup kablosuz, ZigBee ve BLE cihazlarından veri toplama işlemleri ve paket analizi tekniklerini iyileştirme yolları araştırılmıştır (TajDini vd., 2019).

IEEE Transactions on Cognitive Communications and Networking adlı dergide yayınlanan *"No Radio Left Behind: Radio Fingerprinting Through Deep Learning of Physical-Layer Hardware Impairments"* başlıklı makalede, CNN algoritması kullanılarak donanıma özgü kusurlar ve özelliklerin sınıflandırması çalışılmıştır (Sankhe, Belgiovine, Zhou, Angioloni, vd., 2019).

IEEE MILCOM konferansındaki *"Real-time and embedded deep learning on FPGA for RF signal classification"* başlıklı bildiride, gömülü bir yazılım tanımlı radyo platformu olan *DeepRadyo*'nun alan programlanabilir kapı dizisi (FPGA) üzerinde derin öğrenme tabanlı bir RF sinyal sınıflandırıcı tasarlanmış ve RF ön uçtan alınan sinyaller gerçek zamanlı ve düşük güçle farklı modülasyon türlerine göre sınıflandırılmıştır (S. Soltani vd., 2019).

2019 IEEE GC Wkshps çalıştayındaki *"SDR Demonstration of Signal Classification in Real-Time Using Deep Learning"* başlıklı bildiride, gerçek zamanlı olarak sinyal sınıflandırma özelliğine sahip bir yazılım tanımlı radyo (SDR) prototipi gösterilmektedir. Çalışmada kablosuz

sinyal modülasyon sınıflandırması için evrişimli sinir ağı (CNN) kullanılmaktadır (Gravelle ve Zhou, 2019).

IEEE Communications Surveys & Tutorials'ta *"A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security"* başlıklı makalede, IoT sistemleri için gelişmiş güvenlik yöntemleri geliştirmek için kullanılabilecek makina öğrenimi yöntemlerinin ve DL yöntemlerindeki son gelişmelerin kapsamlı bir araştırması yapılmaktadır. Doğal veya yeni ortaya çıkan tehditlerle ilgili IoT güvenlik tehditleri sunulmakta ve çeşitli olası IoT sistem saldırı yüzeyleri ve her yüzeyle ilgili olası tehditler tartışılmaktadır (Al-Garadi vd., 2020).

IJERT'te *"Analysis of RF Device Fingerprinting using Convolutional Neural Network"* başlıklı makalede bir dizi benzer cihaz arasından belirli bir cihazı tanımlamaya yönelik bir yöntem, evrişimli sinir ağı teknikleri kullanılarak tartışılmaktadır. Değişen sinyal-gürültü oranları (SNR'ler) için zaman alanındaki karmaşık temel bant hata sinyallerini kullanarak evrişimli sinir ağını eğitmek için bir çerçeve geliştirilmektedir (Parvathi ve Basu).

IEEE 91st VTC2020-Spring konferansında sunulan *"Deep learning for over-the-air non-orthogonal signal classification"* başlıklı bildiride, LOS (Line-of-sight) ve NLOS (Non-line-of-sight) kanal senaryoları için CNN ile ortogonal olmayan SEFDM sinyalleri için akıllı bir sinyal sınıflandırma işlemi yapılmaktadır (T. Xu ve Darwazeh, 2020).

2020 IEEE Journal of Radio Frequency Identification konferansında sunulan *"A review of radio frequency fingerprinting techniques"* başlıklı derlemede, kablosuz cihazlar için RF parmak izi alma yöntemlerini gözden geçirmektedir. Ayrıca geçici durum tespitinde yaygın olarak kullanılan bazı yaklaşımlar ve bunların avantaj ve dezavantajları incelenmektedir. Ana fikir, taklit edilemez imzalar oluşturmak için kablosuz cihazlardan benzersiz özellikler çıkarmaktır (Soltanieh vd., 2020).

Data'da *"A Database for the Radio Frequency Fingerprinting of Bluetooth Devices"* başlıklı makalede, 27 farklı akıllı telefondan (her biri için birkaç model bulunan altı üretici) farklı örnekleme oranlarında toplanan Bluetooth (BT) sinyallerinden oluşan bir veri tabanı sunulmaktadır. Geçici sinyal tabanlı RFF yönteminde, anlık sinyal karakteristikleri temelinde sinyalin AG'yi, AFr'yi ve AFa'yı olmak üzere üç yüksek mertebeden istatistiksel (HOS) özelliği (skewness, basıklık ve varyans) türetilmektedir (Uzundurukan vd., 2020).

CS & IT konferansında *"Using SDR Platform to Extract The RF Fingerprint of the wireless devices for device identification"* başlıklı çalışmada, Wi-Fi cihazları tarafından iletilen RF sinyallerini ölçmek için düşük maliyetli bir SDR platformu ile yakalanan sinyallerden RF parmak izini çıkarmaktadır. Kablosuz cihazları tanımlamak için RF parmak izi olarak yalnızca güç spektral yoğunluğunu kullanılarak, sınıflandırıcı olarak makina öğrenme modeli kullanılmaktadır (T.-Y. Lin vd.).

IEEE Access dergisindeki *"Performance Assessment of Transient Signal Detection Methods and Superiority of Energy Criterion (EC) Method"* başlıklı makalede, geçici sinyallerin başlangıç noktasını saptamak için çeşitli yöntemler sunulmuştur. Bu yöntemlere alternatif olarak, bu çalışmada Energy Criterion (EC) tekniğini ilk kez kullanan bir yöntem önerilmektedir (Mohamed vd., 2020).

IEEE Internet of Things Magazine'de *"Deep learning for RF fingerprinting: A massive experimental study"* başlıklı makalede, makina öğrenimi tekniklerinin, 400 GB faz içi (I) veri kümesini ve 10.000 radyo tarafından iletilen kareleme (Q) sinyal verisini analiz ederek RF parmak izini nasıl etkilediğini göstermektedir (Jian vd., 2020).

Sensors'te *"On the performance of variational mode decomposition-based radio frequency fingerprinting of Bluetooth devices"* başlıklı makale, Bluetooth (BT) geçici sinyallerinden özelliklerin çıkarılmasında değişken mod ayrıştırmasının (VMD) kullanımının, sınıflandırma doğruluğunu iyileştirmek için etkili bir yol sunduğu gösterilmektedir (Aghnaiya vd., 2020).

Computer Communications'ta *"Deep learning and big data technologies for IoT security"* başlıklı makalede, son teknoloji derin öğrenme, IoT güvenliği ve büyük veri teknolojileri üzerine kapsamlı bir anket gerçekleştirilmektedir. Ayrıca, karşılaştırmalı bir analiz ve derin öğrenme, IoT güvenliği ve büyük veri teknolojileri arasındaki ilişki de tartışılmaktadır. Son olarak, büyük veri teknolojilerini kullanarak IoT güvenliği için derin öğrenmeyi dahil etmenin zorluklarını belirlenmektedir (Amanullah vd., 2020).

Computer Networks'te *"IMSI Catchers in the wild: A real world 4G/5G assessment"* başlıklı çalışmada SDR ile iki açık kaynaklı çerçeve (OpenAirInterface ve SRSLTE) kullanarak IMSI yakalamalarının fizibilitesini ve pratikliğini incelemektedir. Faklı cep telefonu marka/modellerinin davranışını saldırı altında olduklarında değerlendirmektedir (Palamà vd., 2021).

Asilomar Conference on Signals, Systems & Computers konferansındaki *"Radio Frequency Fingerprint Identification for Security in Low-Cost IoT Devices"* başlıklı çalışmada, değişken boyutlardaki giriş sinyallerinin üstesinden gelmek için transformatör tabanlı bir RFFI sistemi önerilmektedir. Çeşitli SNR koşullarında 10 ticari kullanıma hazır LoRa cihazını sınıflandırarak sistemi değerlendirilmektedir. Çevrimiçi artırma, düşük SNR RFFI başarımını %50'ye kadar artırmaktadır (Shen, Zhang, Marshall, Valkama, vd., 2021).

INFOCOM'da *"Radio frequency fingerprint identification for LoRa using spectrogram and CNN"* başlıklı çalışmada, Spektrogram ve evrişimsel sinir ağına (CNN) dayalı uzun menzilli (LoRa) sistemler için bir RFFI (Radyo Frekans Parmak izi Tanımlama) şeması tasarlanmaktadır. Spesifik olarak, LoRa sinyallerinin ince taneli zaman frekansı özelliklerini temsil etmek için spektrogram kullanmaktalar. IQ tabanlı, Fast Fourier dönüşümü tabanlı ve önerdikleri spektrogram tabanlı RFFI şemalarını karşılaştırmaktadırlar (Shen, Zhang, Marshall, Peng, vd., 2021).

Neural Computing and Applications dergisindeki *"Improving security of the Internet of Things via RF fingerprinting based device identification system"* başlıklı çalışmada, RF parmak izi ile mobil ağlarda cihaz tespiti gerçekleştirilmektedir. 4G-LTE haberleşen 5 farklı markanın 10 adet telefonu ile oluşturulan RF veri seti üzerinden 5 farklı makina öğrenimi sınıflandırıcıları ile en yüksek %95,6 başarım elde edilmiştir (Abbas vd., 2021).

Electronics dergisindeki *"Sequential Transient Detection for RF Fingerprinting"* başlıklı çalışmada radyo frekansı parmak izi için sıralı bir geçici algılama yöntemi önerilmiştir. Yöntem, genelleştirilmiş olabilirlik oranı algoritmasının yaklaşık bir uygulamasına dayanmaktadır. Toplamda 16 adet Wi-Fi vericilerinin (3 farklı model) geçici başlangıç noktalarının tesptini, literatürdeki yaklaşımlara göre 20 kat hızlandırmış ve %95'e yakın sınıflandırma başarımı göstermiştir (Taşcıoğlu vd., 2022).

Computer Communications'taki *"Wi-Fi device identification based on multi-domain physical layer fingerprint"* başlıklı çalışmada sinyalin öncü (preamble) kısmından çıkarılan çeşitli çok alanlı özellikleri kullanan cihaz parmak izi alma tekniği önerilmektedir. Random forest modeli kullanılarak, 15 farklı IoT Wi-Fi cihazı türü için %98'e ve aynı tür yongalara sahip 10 ağ kartı için %90,76'ya varan doğruluklar ile parmak izleri belirlenmektedir (Jinghui Zhang vd., 2023).

Literatürdeki çalışmaları doktora tezi ile ilişkilendirdiğimizde, çalışmamızı iki kısımda inceleyebiliriz. İlk kısımda IoT cihazlarının RF parmak izlerini elde etmek için sinyal yakalama süreçlerinde kullanılan donanım, uygulama ve haberleşme protokollerini belirlemek yer almaktadır. Bu kısım için özet bilgi Tablo 1.1'de verilmektedir. Sinyal yakalama süreci tamamlandıktan sonra ise sinyalin belirli durumları (öncül/geçici/kararlı) vasıtasıyla RF parmak izlerinin belirleneceği bölümler ayrıştırılmaktadır (Köse vd., 2019). İkinci kısımda ise belirlenen bu bölümlerden sınıflandırmada kullanılacak öznitelikler belirlenerek geliştirilecek özgün sınıflandırma algoritmaları ile IoT aygıtlarının tanımlanması yapılmaktadır. Tablo 1.2'de literatürde bu alanda kullanılan öznitelikler, sınıflandırma algoritmaları ve bu algoritmaların başarımları verilmektedir.

Tablo 1.1. Literatürdeki RF sinyal yakalama çalışmaları

Referans	Kullanılan SDR veya donanım	Cihaz/Haberleşme Protokolü	Uygulama
(Barbeau vd., 2006)	-	(3COM-4, Ericsson-4, Test Radios-2)/Bluetooth	Matlab
(Ureten ve Serinken, 2007)	Watkins-Johnson model WJ-8633 alıcı, Tektronix TDS3054	IEEE 802.11b 2.4 GHz ISM bandındaki Wi-Fi sinyalleri	-
(Rehman vd., 2012)	PSA E4448A Spektrun Analizörü	Aynı üretici ve modelden iki Bluetooth vericisi	Matlab
(Stewart vd., 2015)	RTL-SDR	FM radio, UHF band sinyalleri, ISM sinyalleri, GSM, GPS ve uydu sinyalleri	Matlab & Simulink
(Nouichi vd., 2019)	HackRF One	Cep Telefonları/GSM	GNU Radio
(J. Yu vd., 2019)	USRP N210	Ti CC2530 ZigBee	Matlab ve Tensorflow
(Ezuma vd., 2019)	Keysight MSOS604A	DJI M100 UAV / -	Matlab
(Peng vd., 2019)	UBX yardımcı kartlarla USRP X310	CC2530 ZigBee	Matlab
(Mohanti vd., 2020)	Ettus B200mini	DJI Matrice M100 UAVs/Airid	Matlab WLAN toolbox
(T.-Y. Lin vd., 2020)	USRP B210	ASUS, Panda, ve TOTO-Link AP/Wi-Fi	XGBoost
(C. Xu vd., 2020)	USRP B210	Hubsan X12, Hubsan X15, Hubsan FPV1/Radiolink AT10	GNU Radio
(Al-Shawabka, Restuccia, D'Oro, & Melodia, 2020)	USRP X310 USRP N210	IEEE 802.11a/g	GNU Radio
(Reus-Muns vd., 2020)	USRP X310, USRP B210	IEEE 802.11a, LTE, 5G-NR	POWDER PAWR platformu (Matlab, GNU Radio)
(Uzundurukan vd., 2020)	Tektronix TDS7404	Akıllı Telefonlar / Bluetooth	Matlab / AWR

(Liu vd., 2020)	USRP B210	ADS-B	Matlab
(D. Huang vd., 2021)	ADALM-PLUTO	ADALM-PLUTO/waveform	Matlab
(L. Chen vd., 2021)	USRP N210	E06-MLE124AP2/Wi-Fi 2.4 GHz	GNU Radio
(Liu vd., 2021)	BladeRF	ADS-B	Matlab
(Jinghui Zhang vd., 2023)	USRP	Wi-Fi (15 farklı IoT cihazı ve 10 adet EW-7811un Edimax ağ kartı)	GNU Radio
(Parmaksız ve Karakuzu, 2022b)	HackRF One	IoT cihazlar (RPi) ve mobil telefonlar	GnuRadio/DragonOS

Tablo 1.2. Literatürdeki RF parmak izi sınıflandırma algoritmaları

Referanslar	Öznitelik/Yöntem	Cihazlar	Sınıflandırma	Başarım
(Ureten ve Serinken, 2007)	Sinyalin anlık özellikleri, temel bileşen analizi (PCA)	WiFi cihazlarından gelen RF dalga biçimleri	Olasılıksal sinir ağı (PNN)	
(Brik vd., 2008)	IQ ofseti, frekans hatası, faz ve büyüklük hatası, senkronizasyon korelasyonu.	802.11 NICs	SVM& k-NN	%99.9 / SVM, %97 / k-NN
(Klein vd., 2009)	Çift ağaç karmaşık dalgacık dönüşümü	Wi-Fi 2 kartlar	Fisher-tabanlı MDA	>=%98 (SNR>=25dB)
(Danev vd., 2009)	Spektral PCA özellikleri, modülasyon şekli	JCOP NXP 4.1 kartları ve e-pasaportlar	Mahalanobis mesafesi	Sınıflandırma:%100, Tanımlama: %97.5
(Danev ve Capkun, 2009)	Varyansa dayalı eşik.	IEEE 802.15.4	Mahalanobis mesafesi.	>=%99.5
(Cobb vd., 2010)	AFa, AFr ve AG (istatistiksel özellikler)	IoT – akıllı kartlar	Çoklu Diskriminant Analizi /Maksimum Olasılık (MDA/ML)	
(Bertoncini vd., 2011)	Dalgacık paket ayrışımı, dinamik dalgacık parmak izi.	Avery-Dennison AD 612ve Runway Gen 2	k-NN, SVM, LDC ve QDC	%99
(Rehman vd., 2012)	Varyansa dayalı eşik.	Bluetooth alıcı-vericileri.	k-NN (STFT ile enerji zarfı elde etme)	%99.9
(M. M. U. Rahman vd., 2014)	Clock Offset Kalman filtreleri	Kablosuz sistemler	Ölçüm-hipotez-filtreleme (MHF)	

(Yuan vd., 2014)	Faz tabanlı.	GSM telefonlar.	SVM	%100
(Y. Huang, 2017)	IQ dengesizliği.	Matlab simulasyon.	SVM	>=%90 (SNR>=15dB)
(Taşcıoğlu vd., 2017)	AG tepkileri (Genlik özellikleri) ve bunların kullanılarak elde edilen boyutsal olarak indirgenmiş biçimleri (PCA özellikleri)	Vericiler	PNN sınıflandırıcısı kNN'den daha iyi performans gösteriyor.	
(Liang vd., 2017)	SEI'de Ampirik Mod Ayrışımı Wigner-Ville dağılımı (WVD)	Mobile telefonlar & WLAN kartlar	SVM	Geçici sinyal >%93 (doğru tanımlama oranı) SNR>0dB
(Ding vd., 2018)	Bispectrum Spesifik emitör tanımlaması (SEI))	E310, B210 & N210	CNN	>%87
(Sankhe, Belgiovine, Zhou, Riyaz, vd., 2019)	IQ dengesizliği ve DC dengesi.	Telefonlar, dizüstü bilgisayarlar ve dronlar	CNN	%98.6 (veri kümesi:(A. Jagannath vd., 2022))
(Ezuma vd., 2019)	Üç aşamalı dalgacık ayrışımı.	micro-UAV kontrolörleri.	k-NN, SVM, DA, nöral ağlar	k-NN %96.3, SVM %96.84
(Peng vd., 2019)	Diferansiyel takımyıldız iz figürü (DCTF)	CC2530 ZigBee modülleri.	CNN	%99.1 (SNR=30dB)
(Reus-Muns vd., 2020)	Zaman alanlı RF sinyali.	POWDER platformunda dört BS.	CNN (üçlü kayıp ile artırılmış)	10 dilim çoğunluk oylaması için %99.98
(N. Soltani vd., 2020)	Çoklu veri patlamaları.	Dji M100 UAV'ler.	CNN	> %99
(Jian vd., 2020)	Zaman alanlı RF sinyali.	Wi-Fi & ADS-B cihazlar.	CNN	Görev 4F, %92,5 (iletim başına ADS-B doğruluğu)
(Al-Shawabka, Restuccia,	Zaman alanlı RF sinyali.	NI N210 ve NI X310	CNN	Eğitim ve test >= %87.41

D'Oro, Jian, vd., 2020)				
(Zong vd., 2020)	RF sinyal tayfı (STFT methodu: RF sinyalinden tayf için)	5 verici simülasyonu.	CNN	%99.7
(Parmaksız ve Karakuzu, 2022a)	RF sinyal istatistiksel özellikler	Wi-Fi-2 (4 adet AP'den alınmış)	AÖM, Kısıtlı-AÖM'ler, Meta-AÖM	RS-AÖM %0.9896, Meta-AÖM %0.9938
(Jinghui Zhang vd., 2023)	Sinyalin Preamble kısmı İstatistiksel ölçümler ve modülasyon kodlama özellikleri ile birleştirilmiş, preamble'dan türetilen dalga biçimi alanı özellikleri.	Grup A, 15 farklı IoT cihazı, B grubu, RTL8188CUS çipli 10 adet EW-7811un Edimax kablosuz ağ kartı	Random forest	Farklı 15 IoT cihazı için %98, aynı çipli 10 ağ kartı için %90.76 başarım.

1.2. Tezin Hipotezi

- Literatüre özgün bir RF veri kümesi kazandırmak.
- IoT cihazları için güvenlik çözümlerinde ilave özellikli donanıma ihtiyaç duymadan kısıtlı kaynaklar ile sinyal yakalamak.
- Açık kaynak yazılımlar ve düşük maliyetli yazılım tanımlı radyolar ile RF sinyal yakalama (MEC) sistemi tasarlamak.
- Literatür destekli özgün öznitelikler belirlemek.
- AÖM tabanlı sınıflandırma algoritmalarını başarımlarını RF parmak izi çalışmalarında uygulamak ve literatüre güncel AÖM tabanlı sınıflandırıcılar kazandırmak.

1.3. Tezin Katkıları

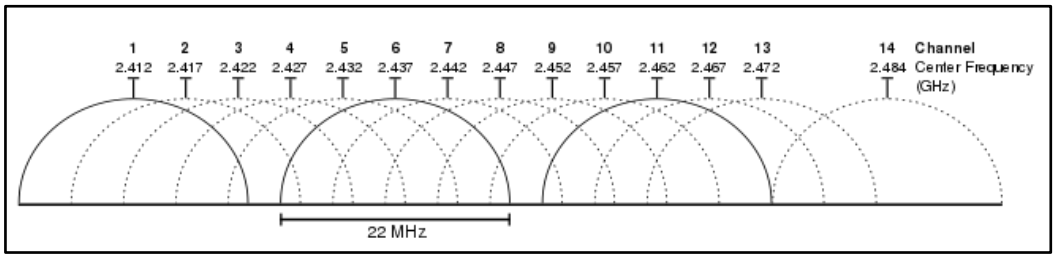
- IoT cihazlarının Wi-Fi sinyalleri, benzersiz bir RF parmak izi veri kümesi oluşturmak için kullanılmaktadır.
- Topluluk tabanlı Meta-AÖM algoritmalarının başarımı, özgün veri kümesi kullanılarak sunulmaktadır
- Temel AÖM olarak ÇK-AÖM kullanan yeni bir Meta-AÖM ağ yapısı (ÇK-Meta-AÖM) geliştirilerek kullanılmaktadır.
- Kısıtlı karma atama Meta-AÖM'ye uyarlanarak başka bir ağ (KK-Meta-AÖM) tanımlanmaktadır.
- Bu çalışma, RF parmak izi tanıma alanında AÖM tabanlı ilk ve tek çalışmadır.

2. IoT FİZİKSEL KATMAN VE RF PARMAK İZİ

RF sinyalleri, kablosuz iletişimde fiziksel katmanda yer alır. OSI (Açık Sistemler Arası) modelinde, fiziksel katman en alt katmandır ve verilerin kablosuz ortam üzerinden iletimini sağlar. Fiziksel katman, veri bitlerinin elektrik, optik veya radyo sinyallerine dönüştürülerek iletim ortamı üzerinden gönderilmesinden sorumludur. Bu katman, verinin nasıl kodlandığı, bitlerin nasıl modüle edildiği, sinyallerin nasıl taşındığı ve ortam üzerinden nasıl iletim yapıldığı gibi işlemleri yönetir.

2.1. IoT Fiziksel Katman

2.4 GHz frekansında yayın yapan cihazlarda on dört kanal belirlenmiştir, kanal 14'ten önceki 12 MHz'lik bir boşluk dışında 1-13 arasındaki kanallar birbirinden 5 MHz aralıklıdır. Dünyanın çoğu, spektrumdaki ilk on üç kanala izin vermektedir. 14. kanal ise Japonya tarafından kullanılmaktadır. Şekil 2.1'de görüldüğü gibi 2.4 GHz frekansında yalnızca üç kanalın (1,6 ve 11) örtüşmeyen frekans alanına sahip olduğu görülmektedir.

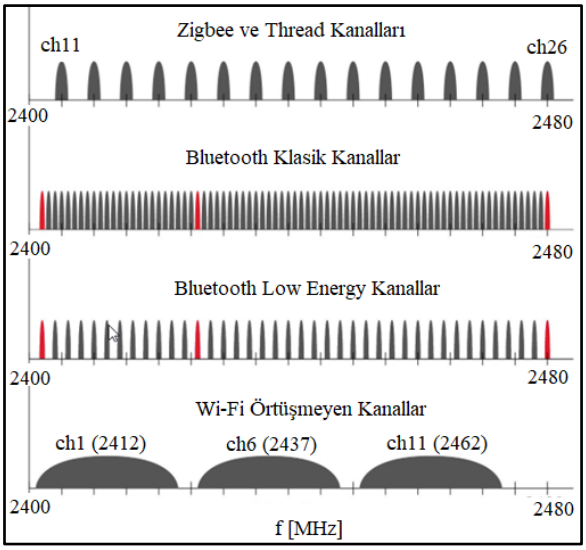


Şekil 2.1. 2.4 GHz bandında örtüşen 20 MHz kanallar

Kaynak: (Moety, 2014)

Wi-Fi birlikteliği, Wi-Fi, ZigBee, Thread ve Bluetooth dâhil olmak üzere birden fazla 2.4 GHz teknolojisinin, bitişik radyolara müdahale eden bir radyodan gelen sinyaller olmadan çalışmasına izin vermektedir (Woodings ve Gerrior, 2005). Şekil 2.2'de birden fazla 2.4 GHz teknolojisini kullanan haberleşme sisteminin frekans tayfı (spektrumu) verilmektedir.

Lisanssız 2.4 GHz ISM bandında radyo frekansı modülasyonu için FHSS ve DSSS olmak üzere iki yöntem vardır. Bluetooth FHSS kullanırken WirelessUSB, 802.11b/g/a (genelde Wi-Fi olarak bilinir) ve 802.15.4 (üst ağ katmanlarıyla birleştirildiğinde ZigBee olarak bilinir) DSSS kullanmaktadır. Bu teknolojilerin tümü, dünya çapında kullanılabilen ISM frekans bandında (2.400-2.483 GHz) çalışmaktadır.



Şekil 2.2. 2.4 GHz protokollerinin frekans çakışması

Kaynak: (Silicon Labs, 2023)

Wi-Fi, her bir kanalın 22 MHz genişliğinde olduğu DSSS'yi kullanmaktadır ve birbiriyle örtüşmeden aynı anda üç eşit şekilde dağıtılmış kanalın kullanılmasına izin vermektedir. Her Wi-Fi erişim noktası tarafından kullanılan kanal elle (manuel) yapılandırılmalıdır. Wi-Fi istemcileri, mevcut erişim noktaları için tüm kanalları aramaktadır. 802.11, orijinal 1 ve 2 Mbit/s veri hızları için her bilgi bitini kodlamak için *Barker kodu* olarak bilinen 11 bitlik bir sahte PN kodu kullanmaktadır. Daha yüksek veri hızları elde etmek için 802.11b, CCK kullanarak altı bilgi bitini sekiz çipli bir sembole kodlamaktadır. Bu CCK algoritmasında kullanılan 64 olası sembol vardır ve her 802.11b telsizinin 64 ayrı korelatör (sembolleri bilgi bitlerine dönüştürmekten sorumlu cihaz) içermesini gerektirir, bu da telsizin karmaşıklığını ve maliyetini artırmaktadır ancak, veri hızını 11 Mbit/s'e çıkarmaktadır.

Bluetooth'un odak noktası, cep telefonları, kulaklıklar ve PDA'lar arasında geçici birlikte çalışabilirliktir. Çoğu Bluetooth cihazı düzenli olarak şarj edilmektedir. Bluetooth, FHSS kullanmaktadır ve 2.4 GHz ISM bandını 79 adet 1 MHz kanallara bölmektedir. Bluetooth aygıtları 79 kanal arasında saniyede 1600 kez sözde rasgele bir düzende atlamaktadır. Bağlı Bluetooth cihazları, piconet adı verilen ağlarda gruplanmaktadır, her *piconet* bir ana ve yedi adede kadar aktif bağımlı içermektedir. Her bir *piconetin* kanal atlama dizisi, ana istemcinin (master) saatinden türetilmektedir. Tüm bağımlı cihazlar bu saatle senkronize kalmalıdır. İleri hata düzeltmesi (FEC), başlıktaki her biti üç kez ileterek tüm paket başlıklarında kullanılmaktadır. Bazı paket türlerinin veri yükünün ileri hata düzeltmesi için bir Hamming

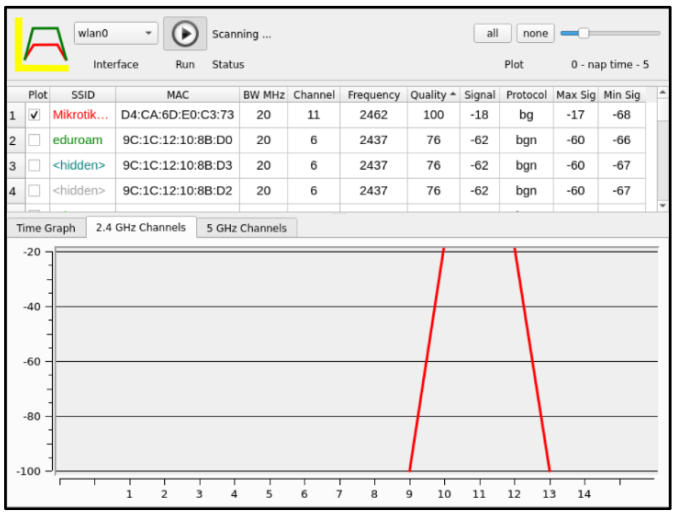
kodu da kullanılır. Hamming kodu, her veri paketine %50 ek yük getirmektedir ancak, tüm tekli hataları düzeltebilir ve her 15 bitlik kod sözcüğündeki tüm çift hataları algılayabilmektedir(her 15 bitlik kod sözcüğü, 10 bit bilgi içerir). Ayrıca, AFH algoritması ile Bluetooth'un Wi-Fi ve WirelessUSB gibi DSSS sistemleri tarafından işgal edilen kanallardan kaçınmasını sağlamaktadır.

ZigBee, sensör ve kontrol ağları için standart bir çözüm olarak tasarlanmıştır. Çoğu ZigBee cihazı, hedef pil ömrü yıllarla ölçüldüğü için son derece güce duyarlıdır (termostatlar, güvenlik sensörleri vb.). ZigBee ayrıca 868 MHz bandında (Avrupa), 915 MHz bandında (Kuzey Amerika) ve 2.4 GHz ISM bandında (dünya çapında mevcut) bir DSSS radyo sinyali kullanmaktadır. 2.4 GHz ISM bandında on altı kanal tanımlanmıştır, her kanal 3 MHz yer kaplar ve kanallar birbirinden 5 MHz uzakta ortalanmakta, bu da kanal çiftleri arasında 2 MHz'lik bir boşluk sağlamaktadır. ZigBee, her bir sembole kodlanmış 4 bilgi biti ile maksimum 128 Kbps veri hızı sağlayan 11 çipli bir PN kodu kullanmaktadır. Fiziksel ve MAC katmanları, IEEE 802.15.4 Çalışma Grubu tarafından tanımlanmakta ve IEEE 802.11b standardı ile aynı tasarım özelliklerinin çoğunu paylaşmaktadır.

2.4 GHz kablosuz telefonlar Kuzey Amerika'da giderek daha popüler hale gelmekte ve standart bir ağ teknolojisi kullanmamaktadır. Bazı telefonlar DSSS kullanmakta çoğu telefon ise FHSS kullanmaktadır. DSSS ve diğer sabit kanal algoritmalarını kullanan telefonlarda, telefonda tipik olarak, kullanıcıların kanalı manuel olarak değiştirmesine olanak tanıyan bir "kanal" düğmesi bulunmaktadır. FHSS telefonlarda sürekli kanal değiştirdikleri için "kanal" düğmesi bulunmamaktadır. Çoğu 2.4 GHz kablosuz telefon, 5 ila 10 MHz kanal genişliği kullanmaktadır.

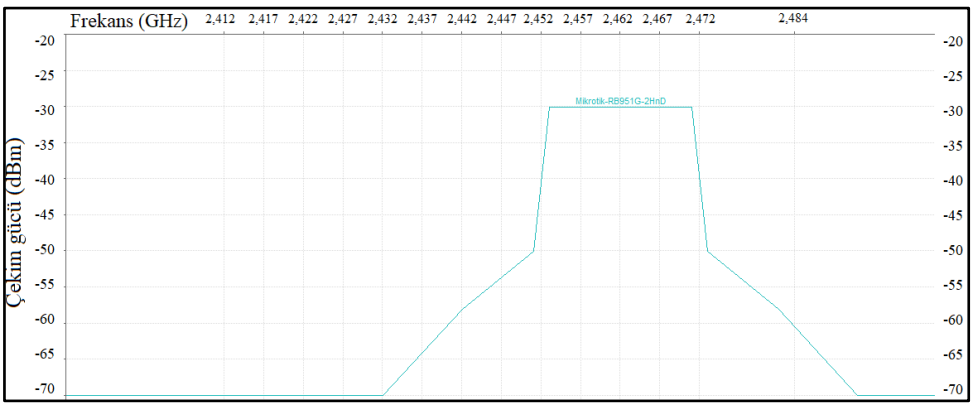
Wi-Fi'nin çarpışma önleme algoritması, iletimden önce sessiz bir kanalı dinlemektedir. Bu, birden fazla Wi-Fi istemcisinin tek bir Wi-Fi erişim noktasıyla verimli bir şekilde iletişim kurmasını sağlamaktadır. Wi-Fi kanalı gürültülüyse, Wi-Fi cihazı, kanalı tekrar dinlemeden önce rastgele bir geri dönüş yapmaktadır. Kanal hala gürültülüyse, kanal sessizleşene kadar işlem tekrarlanmakta kanal sessiz olduğunda, Wi-Fi cihazı iletimine başlamaktadır. Kanal hiçbir zaman sessiz kalmazsa, Wi-Fi cihazı başka bir kanaldaki diğer mevcut erişim noktalarını arayabilmektedir. Aynı veya çakışan kanalları kullanan Wi-Fi ağları, çarpışmadan kaçınma algoritması nedeniyle bir arada var olacak ancak, her bir ağın verimi düşecektir. Aynı alanda birden fazla ağ kullanılıyorsa, kanal 1, 6 ve 11 gibi örtüşmeyen kanalların kullanılması en iyisi olmaktadır. AP cihazları haricinde bilgisayarların işletim sistemi üzerinde yazılım aracılığıyla

Hotspot ile internet paylaşımı amacıyla dinamik kablosuz vericiler oluşturulmaktadır. Şekil 2.3'te açık kaynak LinSSID programı ile 2.4 GHz frekans bandında yayın yapan kablosuz ağlar incelenmektedir.



Şekil 2.3. LinSSID programıyla 2.4 GHz'te yayın yapan AP'lerin analizi

5 GHz frekans bandında 3 farkli (20 MHz, 40 MHz ve 80 MHz) RF kanal bant genişligi mevcuttur. Bant genişliği artışıyla, doğru orantılı olarak hız, termal arkaplan gürültüsü ve enterferansa (kablosuz iletişim sistemlerinde birbirleriyle çakışan veya karışan sinyallerin neden olduğu etkileşimi) açıklık artarken, kapsama alanı ve RF bağlanti kararlılığı azalmaktadır. Bundan dolayı az sayıda AP'nin birbirini duyduğu ortamlarda 80 Mhz kullanılırken, ortam AP sayısı ve istemci sayısı biraz daha yoğunlaşırsa 40 Mhz kullanılmaktadır. Ortam çok yoğun ise mutlaka 20Mhz'e inilmesi gerekmektedir ve RF ortamı bu durumda en kararlıdır. 20 Mhz'de kanal toplam 200 Mbps civari net veri taşıyabildiğinden dolayı istemciler için bu hızlar yeterlidir. Şekil 2.4'te Mikrotik AP'ye ait yayın gücü gösterilmektedir.



Şekil 2.4. Wi-Fi Scanner 22.11 programı ile kablosuz yayın gücünün incelenmesi

IEEE 802.11, bilgisayar haberleşmesinde bir dizi Telsiz Yerel Ağ (TYA / WLAN) standardına verilen isimdir. Bu standart, Elektronik Mühendisleri Enstitüsü (EEME / IEEE) tarafından 1997'den itibaren geliştirilmektedir. EEME'nin 11. çalışma grubu Metropolitan Ağ Standartları (MA / MAN) ile ilgili çalışma yaparken ayrıca 802.11 standardının gelişimi ile ilgilenmektedir. Bu standartta yapılan değişiklikler IEEE 802.11x kavramını temsil etmektedir. 802.11b ve 802.11g'nin diğer değişikliklerden (c-f, h, j) en önemli kabul edilmesi, toplum tarafından daha fazla benimsenmiş ve kullanılmış olmalarıdır. Yapılan değişiklikler ile 802.11 iletişim standardının güvenlik özellikleri ve kapsama mesafesi artmaktadır. Tablo 2.1'de IEEE 802.11 standartlarının yayınlanma tarihleri ile birlikte gelişim evreleri verilmektedir. 802.11 veri bağlantı katmanı iki (üst kısım: IEEE 802.2 Mantıksal Bağlantı Kontrolü (LLC), alt kısım: Medya Erişim Kontrolü (MEK) alt katmana bölünmüştür.

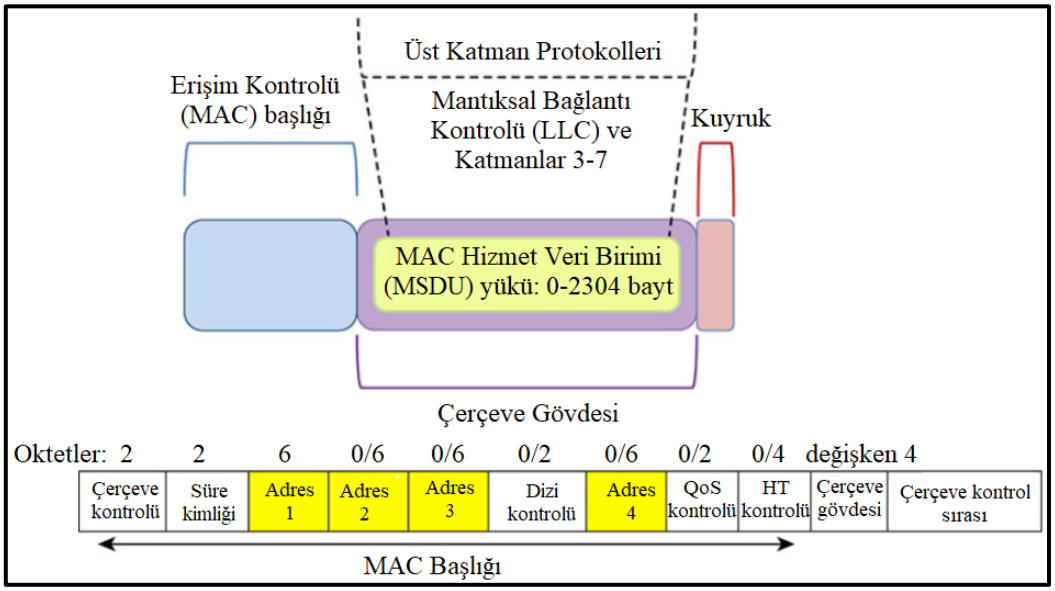
Tablo 2.1. IEEE 802.11 standartları

Yayın tarihi	Standart	Yaygın ad	Frekans (GHz)	Modulasyon türü	Band genişliği (MHz)	Veri hızı (bps)	Yaklaşık aralık (metre)
1997	802.11	Wi-Fi 0	2.4	DSSS, FHSS	22	2 M	20-100
1999	802.11a	Wi-Fi 2	5	DSSS	20	54 M	35-120
1999	802.11b	Wi-Fi 1	2.4	CCK	22	11 M	35-140
2003	802.11g	Wi-Fi 3	2.4	OFDM	20	54 M	38-140
2009	802.11n	Wi-Fi 4	2.4 ve 5	OFDM	20-40	600 M	70-250
2013	802.11ac	Wi-Fi 5	5	OFDM	20-40-160	6.9 G	35-…
2019	802.11ax	Wi-Fi 6	2.4 ve 5	OFDM, OFDMA	80-160	9.6 G	-
2020	802.11ax	Wi-Fi 6E	6	OFDMA	80-160	9.6 G	-
2022'nin 2. yarısında beklenmekte.	802.11be	Wi-Fi 7	2.4, 5 ve 6	OFDMA	320		-

2.2. 802.11 Yönetim Çerçeve Türleri ve Biçimleri

802.11 çerçeveleri üç (başlık, gövde ve kuyruk) ana bölümden oluşmaktadır. MAC Başlığı, çerçeve kontrol bilgisi, süre bilgisi, MAC adresleme, sıra kontrol bilgisi, QoS veri çerçeveleri ve belirli QoS kontrol bilgilerini içermektedir. Çerçeve Gövdesi bileşeninin boyutu değişken olabilir ve çerçeve tipine ve çerçeve alt tipine bağlı olarak farklı bilgiler içermektedir. MSDU üst katman yükü, çerçeve gövdesi içinde kapsüllenmiştir ve katman 3–7 yükü şifreleme kullanılırken korunmaktadır. Kuyruk yani Çerçeve Kontrol Sırası (FCS), alınan çerçevelerin

bütünlüğünü doğrulamak için kullanılan bir 32 bitlik döngüsel artıklık denetiminden (CRC) oluşmaktadır. Şekil 2.5'de detaylı çerçeve biçimi verilmektedir.



Şekil 2.5. Detaylı çerçeve biçimi

802.11 çerçevelerinin *yönetim, kontrol ve veri* olmak üzere üç türü bulunmaktadır. Yönetim çerçeveleri, BSS'yi yönetmektedir. Kontrol çerçeveleri, ortama erişimi kontrol etmektedir. Veri çerçeveleri, katman 3-7 bilgisi olan yükleri içermektedir. Kablosuz ağa katılan cihazların yönetimini sağlamak için *yönetim çerçeveleri* kullanılır. Yönetim çerçeveleri ağa katılan cihazların kimlik doğrulama, bağlantı kurma ve ağdaki diğer cihazların keşfedilmesi gibi işlemleri gerçekleştirir. Kablosuz ağın kontrolünü sağlamak için *kontrol çerçeveleri* kullanılır. Kontrol çerçeveleri veri aktarımını yönetir, veri iletim hatalarını düzeltir ve kablosuz ağdaki diğer cihazların durumunu izler. Kablosuz ağda gerçek veri transferini sağlamak için *veri çerçeveleri* kullanılır. Veri çerçeveleri, kullanıcıların gönderdiği verileri diğer cihazlara iletmek için kullanılır.

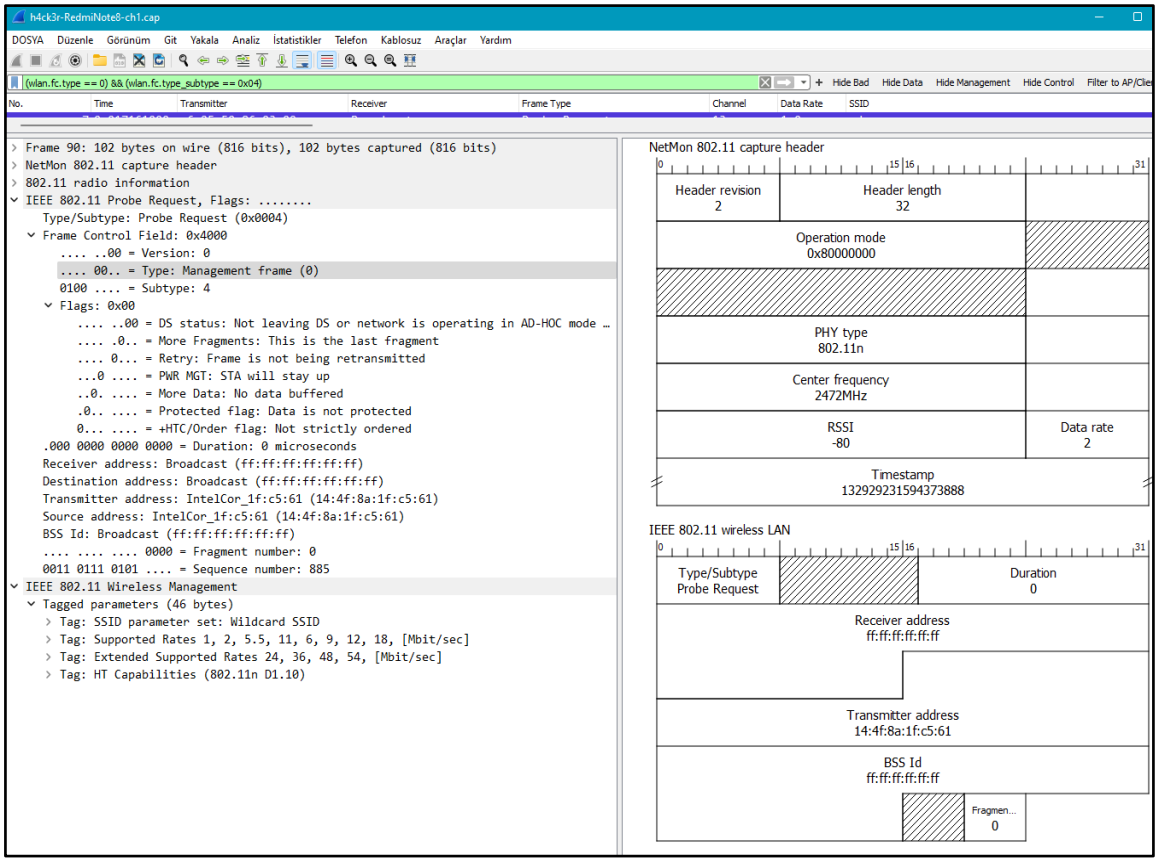
2.2.1. Yönetim çerçeveleri

Her bir çerçeve türü, kablosuz ağdaki belirli bir işlevi gerçekleştirmek için tasarlanmıştır ve 802.11 standardı altında belirtilen protokoller ile yönetilmektedir. Tablo 2.2'de, 802.11-2007 standardı tarafından tanımlanan 12 yönetim çerçevesi alt tipi ve yönetim çerçevesi alt tipleri için Wireshark programında yazılacak filtre örnekleri verilmektedir.

Tablo 2.2. Yönetim çerçeve alt tiplerinin Wireshark programında filtre karşılıkları

Alt tip bitleri	Alt tipler	Wireshark filtre örnekleri
0000	İlişkilendirme isteği (Association request)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x00)
0001	İlişkilendirme yanıtı (Association response)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x01)
0010	Yeniden ilişkilendirme isteği (Reassociation request)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x02)
0011	Yeniden ilişkilendirme yanıtı (Reassociation response)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x03)
0100	Araştırma isteği (Probe request)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x04)
0101	Araştırma yanıtı (Probe response)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x05)
1000	İşaret (Beacon)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x08)
1001	ATIM (announcement traffic indication message)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x09)
1010	Ayrışma/Ayrılma (Disassociation)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x0a)
1011	Kimlik doğrulama (Authentication)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x0b)
1100	Yetkisizlendirme (Deauthentication)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x0c)
1101	Eylem (Action)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x0d)
1110	Eylem hayır onay (Action no ack)	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x0e)

Wireshark uygulaması ile yönetim trafiğini filtrelemek için bu alt türler kullanılmaktadır. Şekil 2.6'da ağ trafiği analiz aracı olarak kullanılan açık kaynak kodlu Wireshark programı ile gerçekleştirilmiş bir araştırma isteği incelenmektedir.



Şekil 2.6. Wireshark programında araştırma isteği örneği

2.2.2. Kontrol çerçeveleri

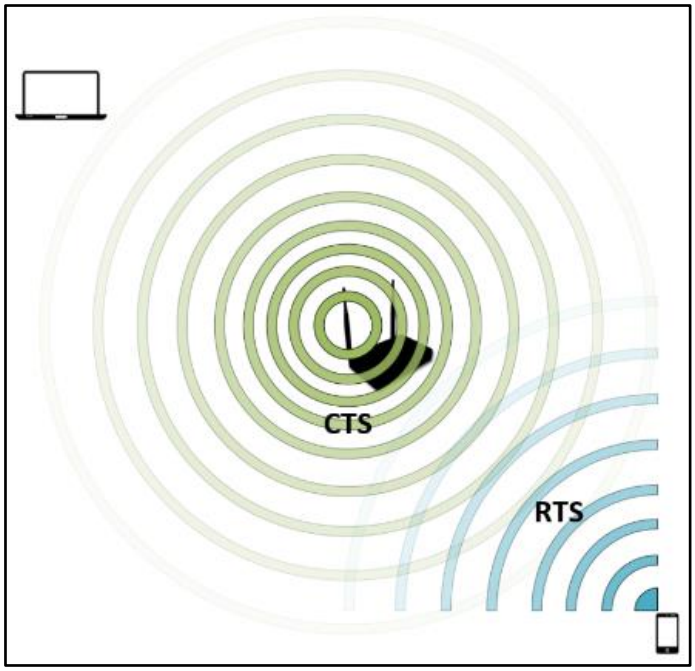
Kontrol Çerçeveleri, ortama erişimi kontrol etmek için ve çerçeve onayı için kullanılmaktadır. Tablo 2.3'te belirtilen kontrol çerçevesi türleri, yalnızca nokta koordinasyon işlevi (PCF) tabanlı kablosuz ağlarda kullanılmaktadır.

Tablo 2.3. Kontrol çerçevesi türleri

Alt tip bitleri	Alt tip açıklaması
0100	Hüzmeleme Raporu Anketi (Beamforming Report Poll)
0101	VHT/HE NDP Anonsu (Announcement)
0110	Kontrol Çerçevesi Uzantısı (Control Frame Extension)
0111	Kontrol sarmalayıcı (Control wrapper)
1000	Block ACK Request
1001	Block ACK
1010	PS-Poll

1011	RTS
1100	CTS
1101	ACK
1110	CF-End
1111	CF-END+CF-ACK

İstasyonlar, ortamı çerçeve başlığındaki süre alanında bulunan mikrosaniye cinsinden süre için ayırmak üzere RTS çerçeveleri göndermektedir. Bir istasyon tarafından gönderilen bir RTS çerçevesine yanıt olarak bir AP tarafından gönderilen çerçeve CTS olarak ifade edilmektedir. CTS mesajları, BSS'deki tüm istasyonlara ulaşmalarını sağlayan zorunlu en düşük veri hızında gönderilir. Başlıkta yalnızca alıcı adresi (RA) alanını kullanırlar. Alıcı adres alanındaki istasyon, çerçeve gönderecek olan istasyondur. Şekil 2.7'de RTS ve CTS çerçevelerinin durumu gösterilmektedir.



Şekil 2.7. İstasyon ve AP iletişiminde kullanılan çerçeveler.

2.2.3. Veri çerçeveleri

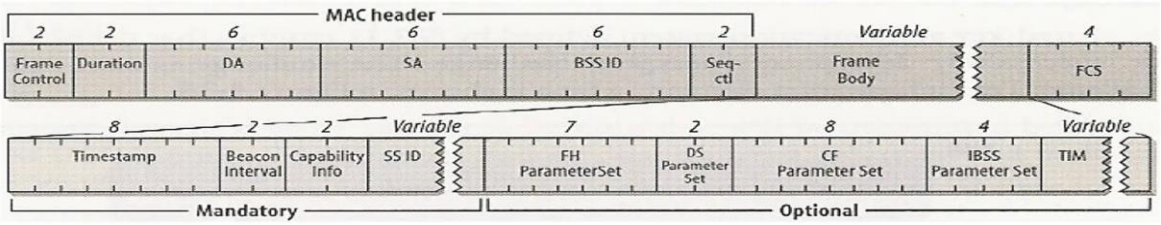
Veri çerçeveleri, bilgi aktarmak veya bir olayı tetiklemek için kullanılır. Tüm veri çerçeveleri bir yük içermez, bazıları "boş veri çerçeveleridir" ve yalnızca bir başlık ve son bilgi içerir. Tablo 2.4'te belirtilen veri çerçevesi türleri, yalnızca HCF kontrollü kanal erişimi (HCCA) veya nokta koordinasyon işlevi (PCF) tabanlı kablosuz ağlarda kullanılmaktadır.

Tablo 2.4. Veri çerçevesi türleri

Alt tip bitleri	Alt tip açıklaması
0000	Data
0001	Data + CF-ACK
0010	Data + CF-Poll
0011	Data + CF-ACK + CF-Poll
0100	Null (no data)
0101	CF-ACK (no data)
0110	CF-Poll (no data)
0111	CF-ACK + CF-Poll (no data)
1000	QoS Data
1001	QoS Data + CF-ACK
1010	QoS Data + CF-Poll
1011	QoS Data + CF-ACK + CF-Poll
1100	QoS Null (no data)
1101	Reserved
1110	QoS CF-Poll (no data)
1111	QoS CF-ACK + CF-Poll (no data)

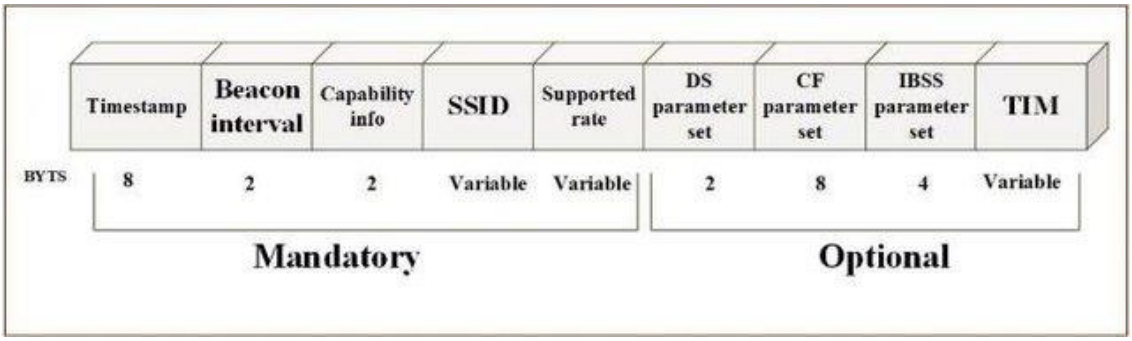
a) 802.11 Yönetimi: İşaret Çerçevesi (beacon frame)

802.11 standardı altında kullanılan yönetim çerçeveleri arasında "beacon frame" de bulunur (Nyathi ve Ndlovu). Beacon çerçeveleri, kablosuz ağların genel olarak kullanımı ile ilgili bilgileri diğer cihazlara duyurmak için kullanılır. Şekil 2.8'de işaret çerçevesnin genel yapısı, Şekil 2.9'da ise işaret çerçevesinin alanları ve bu alanlara ait bayt cinsinden işgal ettikleri bölgeler gösterilmektedir.



Şekil 2.8. İşaret çerçevesinin genel yapısı

Kaynak: (RF Wireless World, 2023)



Şekil 2.9. İşaret çerçevesinin vücut kısmı

Kaynak: (Alsahlany vd., 2018)

Beacon çerçeveleri, bir kablosuz erişim noktasından yayınlanır ve ağa katılmak isteyen cihazlar tarafından algılanır. Bu çerçeveler, ağın adı (SSID), erişim noktasının MAC adresi, ağın kanal numarası, güvenlik ayarları, hizmet seti tanımlayıcısı (BSSID) ve belirli bir hizmet setinde kullanılan diğer parametreleri içerebilir. Beacon çerçeveleri, ağın yönetimi için önemlidir çünkü ağa katılmak isteyen cihazlar tarafından algılanarak ağa katılma taleplerini oluştururlar. Ayrıca beacon çerçeveleri, ağın durumu hakkında bilgi vererek ağa bağlı cihazların hangi kanalda çalışması gerektiği gibi konularda da yol gösterici olurlar. Beacon çerçeveleri, ağ yönetimi için önemli olduğu kadar bazı saldırılar için de kullanılabilirler. Örneğin, bir saldırgan, beacon çerçevelerini kullanarak sahte bir erişim noktası oluşturabilir ve bu noktaya bağlanmaya çalışan cihazları hedefleyebilir. Bu nedenle ağ yöneticilerinin güvenliği sağlamak için beacon çerçevelerini dikkatle izlemeleri ve ağlarını koruma altına almaları önemlidir.

Tablo 2.5'te beacon çerçevelerini oluşturan alanlar/bileşenler, *Frame Control, Duration/ID, Receiver Address, Transmitter Address, Destination Address, Source Address, Fragmentation Number, Sequence Number, Timestamp, Beacon Interval ve Capabilities Information* olarak verilmektedir.

Tablo 2.5. Beacon çerçevelerini oluşturan alanlar

Alan Adı	İlgili alanin içeriği
Frame Control	Çerçevenin türü ve alt tipi gibi bilgileri içerir. Bu kısım kablosuz ağdaki herhangi bir çerçevenin sahip olduğu standart bilgileri içerir.
Duration/ID	Çerçevenin erişim noktasının (AP) ve cihazların erişim süresi hakkında bilgi içerir.
Receiver Address	Çerçevenin yönlendirildiği cihazın MAC adresini içerir.
Transmitter Address	Çerçevenin gönderildiği cihazın MAC adresini içerir.
Destination Address	Çerçevenin gönderildiği cihazın MAC adresini içerir.
Source Address	Çerçevenin kaynak cihazın MAC adresini içerir.
Fragmentation Number	Çerçevenin bölümlerinin sayısını belirtir.
Sequence Number	Çerçevenin gönderilen parçalarının sırasını belirtir.
Beacon Interval	Erişim noktası tarafından yayınlanan beacon çerçeveleri arasındaki zaman aralığını belirtir.
Capabilities Information	Erişim noktasının kablosuz ağ özelliklerini ve desteklediği güvenlik protokollerini belirtir

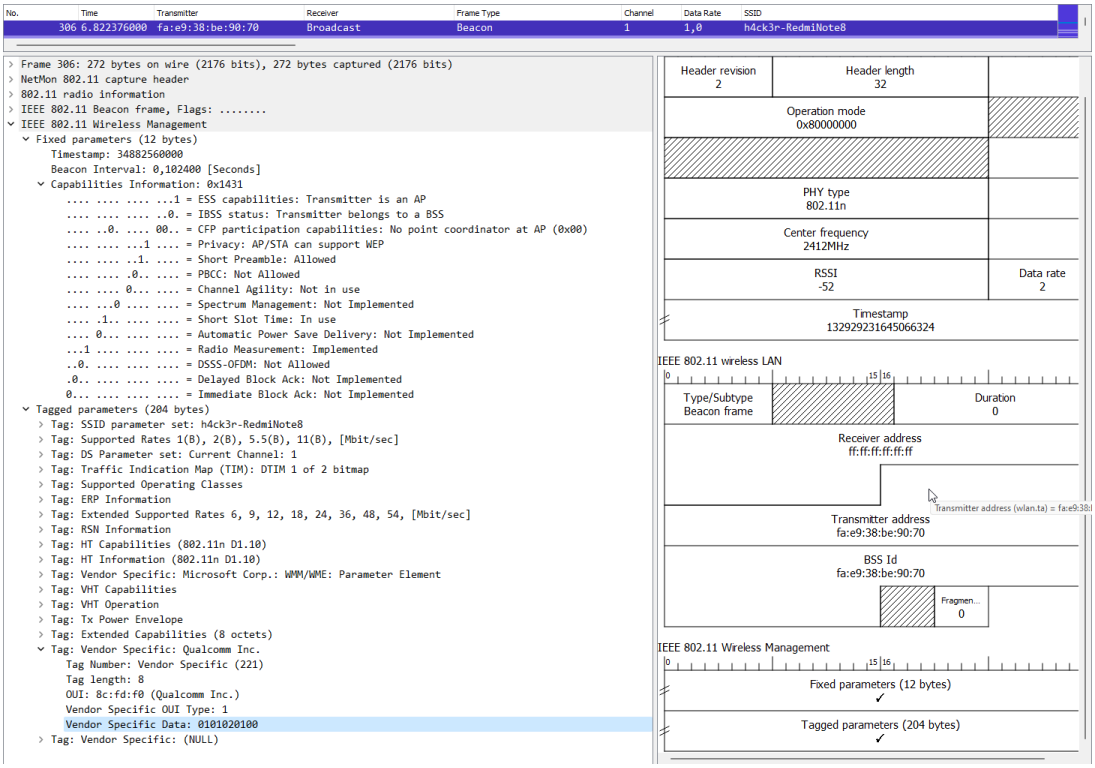
Beacon frame'in çerçeve gövdesi (frame body) bölümünde birkaç zorunlu alan bulunur:

Timestamp (8 bayt): Beacon çerçevesinin gönderildiği zamana dair bilgi içerir. Bu bilgi kablosuz ağlarda senkronizasyonu sağlamak için kullanılır.

Beacon Interval (2 bayt): Erişim noktasının (AP) beacon çerçevelerini ne sıklıkla yayınlayacağını belirten bir zaman aralığıdır. Bu, kablosuz cihazların ağı daha iyi takip etmelerine yardımcı olur.

Capabilities Information (2 bayt): Erişim noktasının kablosuz ağ özelliklerini ve desteklediği güvenlik protokollerini belirtir. Bu bilgi, cihazların ağa katılmadan önce gerekli ayarları yapmasına yardımcı olur.

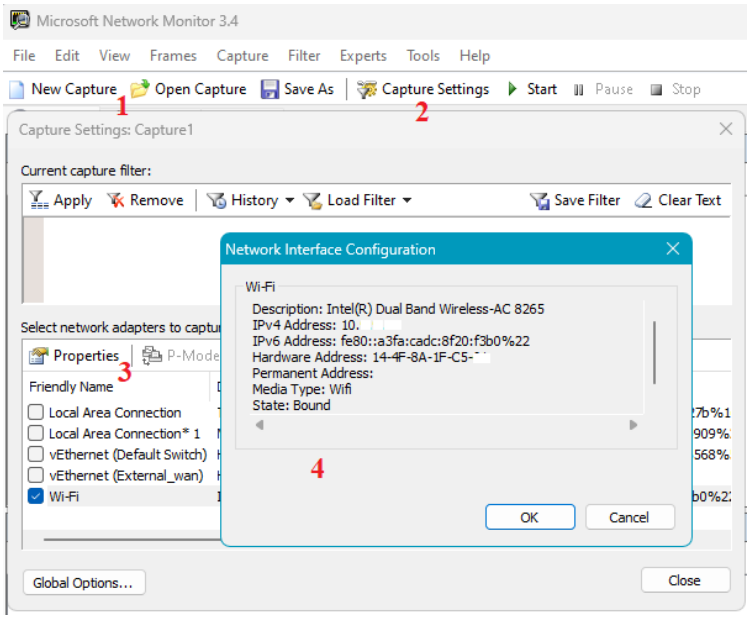
Şekil 2.10'da hotspot yayın yapan bir akıllı telefona ait beacon çerçevelerinin Wireshark ile analizi gösterilmiştir.



Şekil 2.10. Hotspot modunda beacon çerçeve detayı örneği

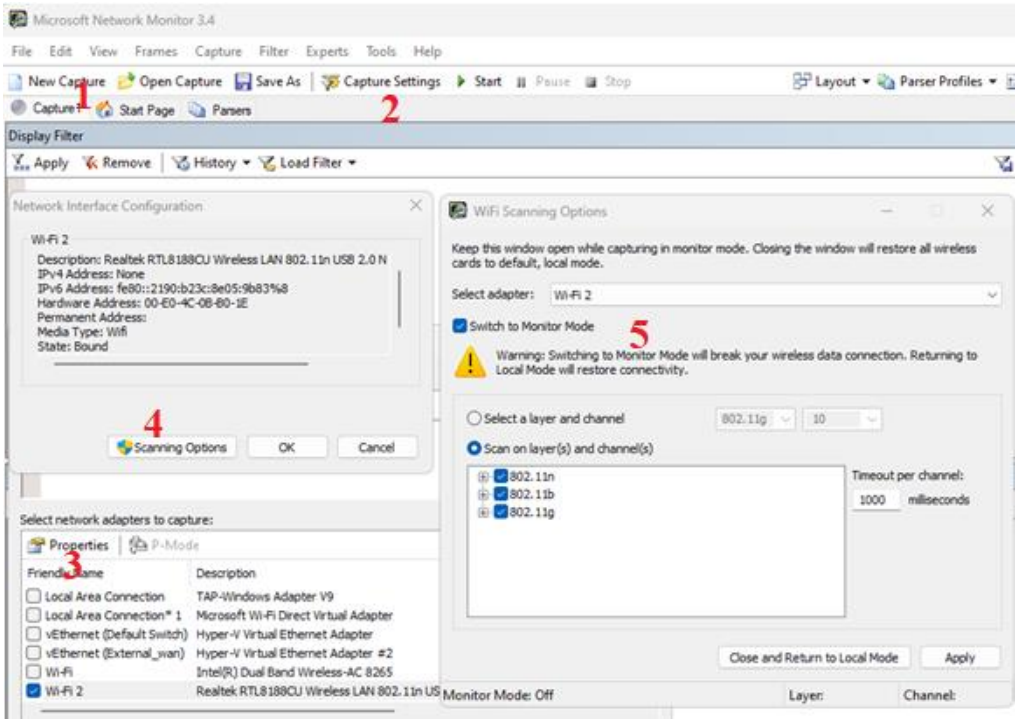
Beacon frame'in çerçeve gövdesinde ayrıca opsiyonel alanlar da bulunabilir. Örneğin, SSID (Service Set Identifier), kanal numarası ve BSSID (Basic Service Set Identifier) gibi bilgiler de beacon frame'in çerçeve gövdesinde yer alabilir. Beacon frame akışını Layer2'de yakalamak için monitör mode desteği olan bir kablosuz alıcı kullanılmaktadır.

Şekil 2.11'de Microsoft Network Monitor 3.4 yazılımıyla Windows 11 işletim sistemi üzerinde aktif bir alıcının monitör mode ayarlarının yapılandırması gösterilmektedir. IE'nin boyutu parantez içinde belirtilmişse, bu elemanlar sabit uzunluktadır. Diğer öğelerin boyutu değişkendir. Beacon Frame'i analiz etmek için Wireshark uygulaması ve MetaGeek Profile (v2.0) kullanılmaktadır.



Şekil 2.11. Microsoft Network Monitor 3.4 yazılımı arayüzü

Şekil 2.11'de ilgili yazılım kullanılarak Wi-Fi kartının monitor modunda yapılandırma adımları verilmektedir. Fakat ilgili Wi-Fi kart monitor modu desteklemediği için, DN-7042-1 gibi usb kablosuz kapsam genişletici cihazlar kullanılmaktadır. Şekil 2.12'de ise monitor mod destekli DN-7042-1'ye ait tarama yapabileceği kanal ve ayarlar verilmektedir.



Şekil 2.12. DN-7042-1 kablosuz USB adaptör ile monitor mod ayarı

SSID: Ağın adını belirten bu alan, istasyonların doğru ağa bağlanmasına yardımcı olur. Tüm İşaretlerde, araştırma taleplerinde, araştırma yanıtlarında, ilişkilendirme talebinde ve yeniden ilişkilendirme taleplerinde bulunur. Öğe Kimliği, SSID IE için 0'dır. SSID maksimum 32 karakter olabilir.

Desteklenen Oranlar (Supported Rates): Bu alan, istasyonların desteklediği veri oranlarını belirtir. Bu alan, ağ yöneticilerinin istasyonların hangi hızlarda veri aktarabileceğini belirlemelerine yardımcı olur. Bu, Beacons, Probe Req, Probe Res, Association Req, Association Res, Reassociation Req ve Reassociation Response'da mevcuttur. Her sekizlinin desteklenen tek bir hızı tanımladığı 8 oktet alanıdır. Her sekizlinin son biti (7.), veri hızının "temel hız veya zorunlu" veya "desteklenen hız" olduğunu gösterir. 7. bit değeri 1 ise temel bir hızı belirtirken, değer 0 ise desteklenen bir hızı belirtir. Sonraki 7 bit (0-6), veri hızı değerini 500kbps birimlerinde belirtir. Şekil 9'da Supported Rates ve Extended Supported Rates alanları mevcuttur. Örneğin: 6 Mbps (12 x500kbps birim) Temel Hız değeri 1001100 olarak gösterilmektedir.

7. bit =1 (temel hızı belirtmek için)

0-6 = 001100 (6 Mbps'yi belirtmek için 12 değeri)

AP tarafından en az bir zorunlu oran belirlenmeli ve hücreye katılmak isteyen herhangi bir istasyon tüm temel oranları desteklemelidir. Verilen örnek birleştirilmiş istasyonun tüm modülasyon tekniklerini (örneğin, BPSK - 6,9 Mbps / QPSK - 12,18 Mbps / QAM - 24Mbps ve üstü) anlamasını sağlamak için 6 Mbps, 12Mbps ve 24Mbps'nin "Temel Hızlar" olarak ayarlandığı varsayılan 802.11a radyo ayarını göstermektedir.

FH parametre seti: Eski Frekans Atlamalı (FH) istasyonları tarafından kullanılır.

DS Parametresi (2 bayt): İstasyonlar tarafından Madde 15, 18 veya 19 PHY kullanılarak oluşturulan beacon çerçevesi ile veya beacon, maddelerden biri tarafından tanımlanan oranlardan biri kullanılarak gönderilirse sunulur.

CF Parametresi (8 bayt): PCF ile kullanılır, gerçek ağlarda kullanılmaz.

BSS parametresi (4 bayt): Yalnızca IBSS'deki (veya Add-Hoc ağındaki) istasyonlar tarafından oluşturulan işaret çerçevelerinde bulunur.

TIM (Trafik Gösterge Haritası): Yalnızca AP'ler tarafından oluşturulan işaret çerçevelerinde bulunur. TIM öğesi, düşük güç modundaki istasyonlar için yararlı bilgiler içerir. AP, arabelleğe

alınmış yayın veya çok noktaya yayın çerçeveleri olup olmadığını hücreye bildirmek için Teslimat Trafiği Gösterge Haritasını (DTIM) kullanır. DTIM, tüm işaretlerde ve tüm TIM'lerde mevcut değildir.

Ülke (Country): Her ülkenin düzenleyici etki alanlarında izin verilen kanalları veya güç seviyelerini sınırlayan düzenleyici organları vardır. İzin verilen kanallar ve maksimum iletim gücü ile birlikte operasyon ülkesini tanımlar. Bu, bir işaretçide zorunlu bir alan değildir.

FH Parametreleri ve FH Model tablosu (Eski FH istasyonları tarafından kullanılır).

Güç Kısıtlaması (Power Constraint) (3 bayt): Bu öğe 802.11h ile ilgilidir. Bu, spektrumun sivil havaalanı radarı, hava durumu radarı gibi diğer amaçlar için kullanıldığı UNII2 ve UNII-2 genişletilmiş (CH52,56,60,64 & CH100-139) içindir. Bu nedenle, bu sistemlerle etkileşimi önlemek için AP, bu kısıtlama alanları tarafından belirtilen maksimum gücü çalıştırmalıdır.

Kanal Anahtarı (6 bayt): Bu aynı zamanda 802.11h ile de ilgilidir. Bir radar patlaması tespit edildiğinde, tüm istasyonlar etkilenen kanalı terk etmelidir. AP, bir sonraki kanal olan hücreye duyuru yapacak şekilde ayarlanabilir.

Quite (8 bayt): Bir AP'nin, kanalı radarların varlığı için test etmek için hiçbir istasyonun iletim yapmaması gereken sessiz bir süre talep edebileceği 802.11h ile ilgili başka bir öğedir.

TPC Raporu (4 bayt): Bu öğe ayrıca, 802.11h ile ilgilidir. TPC Raporu öğesi, genellikle bir TPC Talebi öğesine yanıt olarak gönderilen İletim Gücü ve Bağlantı Marjı bilgilerini içerir.

ERP Bilgileri (3 bayt): ERP öğesi yalnızca 802.11g'yi destekleyen 2.4GHz ağda bulunur ve işaret ve prob yanıtlarında bulunur. ERP_Present olmayan bit, aşağıdaki koşullarda 1'e ayarlanır:

RSN– Sağlam Güvenli Ağ: İstasyonların Kimlik Doğrulama Şifresi, Şifreleme Şifresi ve diğer RSN yeteneklerini belirtmek için kullanılan RSN bilgi öğesi. Aşağıdaki RSN IE'de, Kimlik Doğrulama Paketleri olarak AP desteği 802.1X ve 802.11r FT'yi gösterir. Ayrıca AES'yi ikili şifre (tek noktaya yayın trafiği için) ve grup şifresi (yayın/çoklu yayın için) olarak kullanır.

HT Yeteneği – (HT Operation): 802.11n'de kullanılır.

VHT Yeteneği – (VHT Operation) VHT İletim Gücü Zarfı: 802.11ac'de kullanılır.

Bluetooth iletiminin atlamalı yapısı nedeniyle Bluetooth'tan kaynaklanan parazit asgaridir. Bir Bluetooth cihazı, bir Wi-Fi cihazı “göndermeden önce dinle” yaparken Wi-Fi kanalıyla örtüşen bir frekansta iletim yapıyorsa, Wi-Fi cihazı rastgele bir geri dönüş yapacak

ve bu sırada Bluetooth cihazı, Wi-Fi cihazının iletimine başlamasına izin verecek şekilde örtüşmeyen bir kanala atlayacaktır.

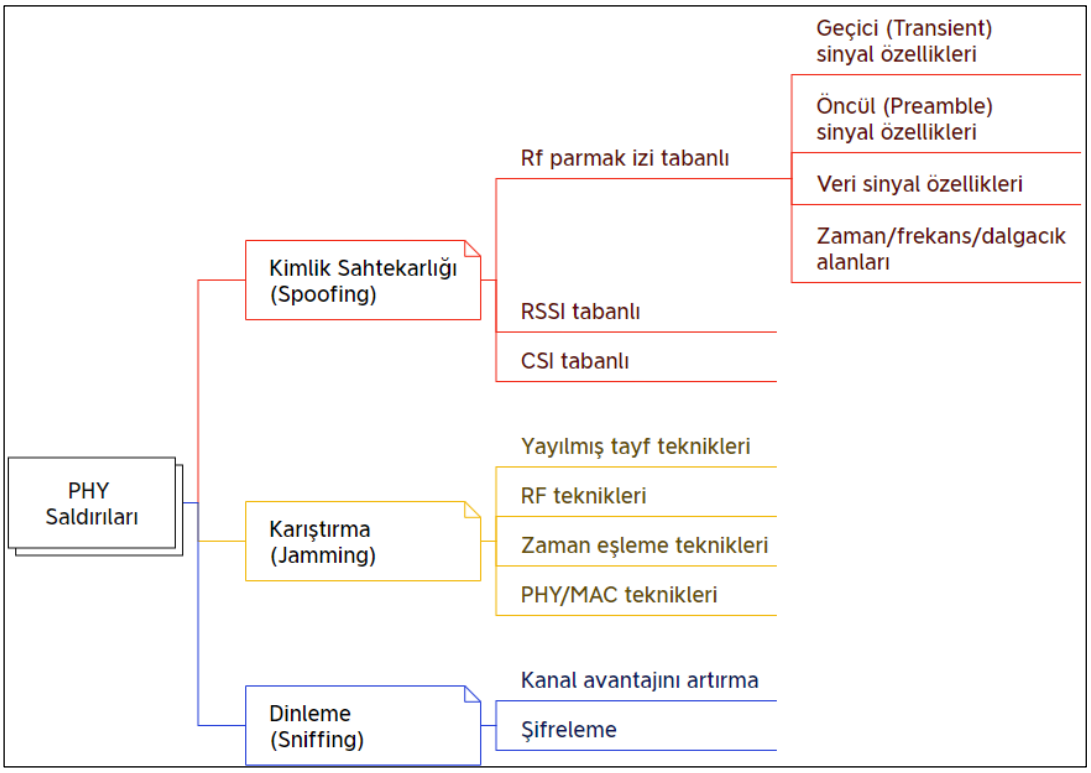
2.4 GHz kablosuz telefonlardan kaynaklanan parazit, kablosuz telefonlar DSSS yerine FHSS kullanıyor olsa bile bir Wi-Fi ağını tamamen durdurabilmektedir. Bunun nedeni kısmen Bluetooth (1 MHz) ile karşılaştırıldığında daha geniş kanal (5 ila 10 MHz) ve ayrıca kablosuz telefon sinyalinin daha yüksek güce sahip olmasından kaynaklıdır. Bir Wi-Fi kanalının ortasına atlayan bir FHSS kablosuz telefon, Wi-Fi iletimini bozarak Wi-Fi cihazının iletimini tekrarlamasına neden olabilmektedir. 2.4 GHz FHSS kablosuz telefonlar büyük olasılıkla yakınlardaki tüm Wi-Fi cihazlarıyla etkileşime neden olmaktadır bu nedenle, bu telefonların Wi-Fi ağları çevresinde kullanılması önerilmemektedir. Telsiz telefon DSSS ise telsiz telefon ve Wi-Fi erişim noktası tarafından kullanılan kanallar çakışmayacak şekilde yapılandırılabilmekte, böylece parazit ortadan kalkmaktadır.

DSSS sistemleri, başka bir DSSS sistemiyle örtüşme tehlikesi nedeniyle kaybedecek en fazla şeye sahip olmaktadır. Ancak, FHSS sistemlerinin frekans çevikliğini elde etmek için DSSS sistemlerinin yapabileceği şeyler bulunmaktadır. Bu yaklaşım, ağ izlemedir. DSSS sistemi bir yoklamalı protokol kullanıyorsa (belirli aralıklarla paketlerin beklendiği yerde), o zaman master, bir dizi başarısız gönderme girişiminden veya kötü alınan paketlerden sonra kanalları değiştirebilir. Diğer bir yaklaşım, radyonun bu özelliği varsa, yayındaki enerji seviyesinin bir okumasını yapmaktır. Havadaki enerji miktarını proaktif olarak ölçmek için bir RSSI kullanılabilir ve bu seviye belirli bir süre içinde çok yüksekse, daha net bir kanala geçilir. Bir FHSS sistemi geçiyorsa kanalların değişmemesi için bir süre dikkate alınır. Bir tarafın alıcı-verici ve bir tarafın alıcı olduğu bir DSSS sisteminde, frekans çevikliğini elde etmek için çoklu iletim yaklaşımı kullanılabilmektedir. Verici, aynı paketi birden fazla frekansta gönderir ve alıcı, alma kanalları arasında çok daha yavaş bir hızda dönmektedir. Bu sistem, alıcı güce bağlıyken ve pille çalışan verici daha az frekansta kullanıldığında çalışmaktadır. Bir kablosuz uzaktan kumanda bu yaklaşımı kullanabilmektedir.

2.3. Güvenlik için Fiziksel Katman Teknikleri

IoT'de kablolu sistemler, karmaşık ve gürültülü yayılma koşullarındaki sağlamlıkları nedeniyle endüstriyel alanda daha hakimdir. İletişim sistemini çökertmeyi veya sistemi kontrol altına almayı amaçlayan kötü niyetli saldırganlara karşı da dayanıklık gösterir. Ancak, kablolu sistemler ciddi bakım, ölçeklenebilirlik ve operasyonel esneklik sınırlamalarına sahiptir.

IoT'de kablosuz sistemler bir çözüm oluşturur, ancak güvenilirlik ve güvenlik açısından performans zayıflıkları gösterir. PHY güvenlik teknikleri kimlik sahtekârlığı, karıştırma ve dinleme saldırılarını temel alır. Kimlik sahtekârlığı ve Dinleme, genellikle çapraz katmanlı bir güvenlik yaklaşımı gerektirir (bkz. Şekil 2.13), çünkü temel koruma yaklaşımları, kimlik doğrulama ve şifreleme, MAC ve üst katman işbirliğini gerektirir (Angueira vd., 2022). Kablosuz iletişimde dinleme saldırılarını önlemenin çözümü ITS'dir. Kimlik sahtekârlığı için PHY karşı önlemleri, her bir kablosuz iletişim bağlantısının benzersiz özelliklerinden yararlanır. Karıştırma saldırılarını önlemek için, Radyo frekansı, Yayılmış Spektrum, Zaman Senkronizasyonu ve Kombine PHY/MAC teknikleri kullanılır. Kimlik, her bir cihazın benzersiz donanım parmak izleri kullanılarak tanımlanabilir (Junqing Zhang vd., 2016). Titreme (Baldini ve Steri, 2017), darbe rampası özellikleri (Baldini ve Steri, 2017), saatler (Danev vd., 2012), geçici durumlar (Ureten ve Serinken, 2007), dalga biçimi bozuklukları (Danev vd., 2012), modülasyon (Brik vd., 2008) veya bunların bir bileşimidir.



Şekil 2.13. PHY katmanı güvenlik teknikleri

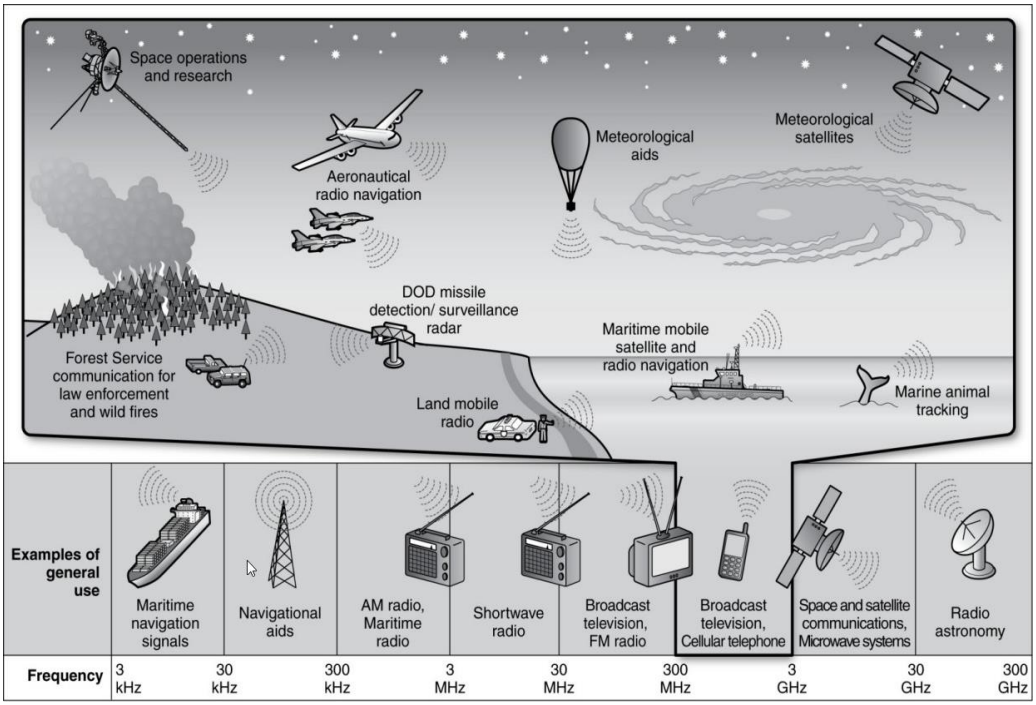
Kaynak: (Angueira vd., 2022)

2.4. RF Parmak İzi

Kablosuz vericilerin üretim aşamasından kaynaklanan sinyal üretici devrelerinde yer alan analog bileşenlerin birbirinden farklı ve taklit edilmesi oldukça zor olan donanım kusurları vardır. Dolayısıyla, her bir verici cihazın iletim sinyallerine yansıyan bu kusurları temel alınarak RF parmak izleri oluşur. Sinyalleri ayırmak için birçok teknik kullanılabilir ancak, hangi tekniğin en uygun olduğu hususu sinyallerin türüne ve gürültü oranına bağlı olarak (sinyallerin sürekli veya kesikli olduğu, analog veya dijital olduğu, tekli veya çoklu olduğu gibi) değişmektedir.

Sinyallerin karşılaştırılması, ölçeklendirilmesi, filtrelenmesi, örnekleme veya modülasyon gibi işlemler yaparak sinyaller arasındaki farklar algılanmaktadır. Sinyallerin frekans aralığını kullanarak, istenmeyen frekanslardaki gürültüyü azaltmak için *filtrelemele* kullanılmaktadır. İstenen sinyali tanımlayan bir *eşleme* filtresi oluşturarak, sadece ilgili sinyal algılanmaktadır. *Çoklu erişim teknikleri* (MAC), birden fazla kullanıcının aynı frekans aralığında veri aktarmasını sağlamaktadır. Sinyallerin *ölçekleri* kullanılarak (ölçeklendirme), sinyaller arasındaki farklılıkları algılanmaktadır.

Doğal elektromanyetik radyasyon tayfının bir parçası olan Şekil 2.14'te verilen RF tayfı 3 kHz ile 300 GHz frekans değerleri arasındadır. Cep telefonları, radyo ve televizyon yayınları gibi kablosuz sistemlerin kullandığı tayf kritik frekans aralığındadır. Bu tayf, [225 MHz ila 3.7 GHz] aralığındaki frekansları kapsar.



Şekil 2.14. Özel tayf kullanımları ve federal tayf kullanımları

Kaynak: (Skorup, 2013)

Ses algılayıcıları, benzersiz varyasyonları ve sesin bazı yönlerini kullanarak konuşmacıyı tanımlar. RF parmak izi bu bağlamda insan konuşmasını taklit edebilir. RF parmak izi, çeşitli radyo ve kablosuz cihazları otomatik olarak tanımlamak için sinyalin zaman/frekans alanı özelliklerini kullanır. Hemen hemen tüm mevcut ve gelecek kablosuz iletişim standartları, ortogonal frekans bölmeli çoğullamayı (OFDM) kullanır (Bloessl vd., 2013).

Sinyalin hangi özellikleri yaygın olarak çıkarılır ve hangi sonuçlara varılır aşağıda açıklanmıştır. RF parmak izi yakalamada (Vo-Huu vd., 2016), SDR platformunu kullanır. Scrambling seed (Descrambler'dan), örnekleme frekansı kayması (Channel Estimator'dan), taşıyıcı frekans kayması ve çerçeve geçişi, (OFDM Synchronizer'dan) çıkarılan ana özelliklerdir. Makalenin sonucuna göre, sonuçlar Wi-Fi cihazlarını tanımlamanın mümkün olduğunu gösteriyor. Ve (Peng vd., 2018), SDR platformunu kullanarak ZigBee cihazlarında RFF yürütmüştür. Bu çalışmada, diferansiyel takımyıldız iz figürü (DCTF), taşıyıcı frekans kayması (CFO), modülasyon kayması ve I-Q kayması özellikleri elde edilmektedir.

Güç spektral yoğunluk (PSD) katsayıları (Rehman, Alam, vd., 2014)'te kullanılmaktadır. Üst düzey alıcıların yüksek performansı nedeniyle RFF tanımlanırken tanımlama doğruluğunun kesinlikle alıcı ile ilgili olduğu vurgulanmaktadır. PSD katsayılarının

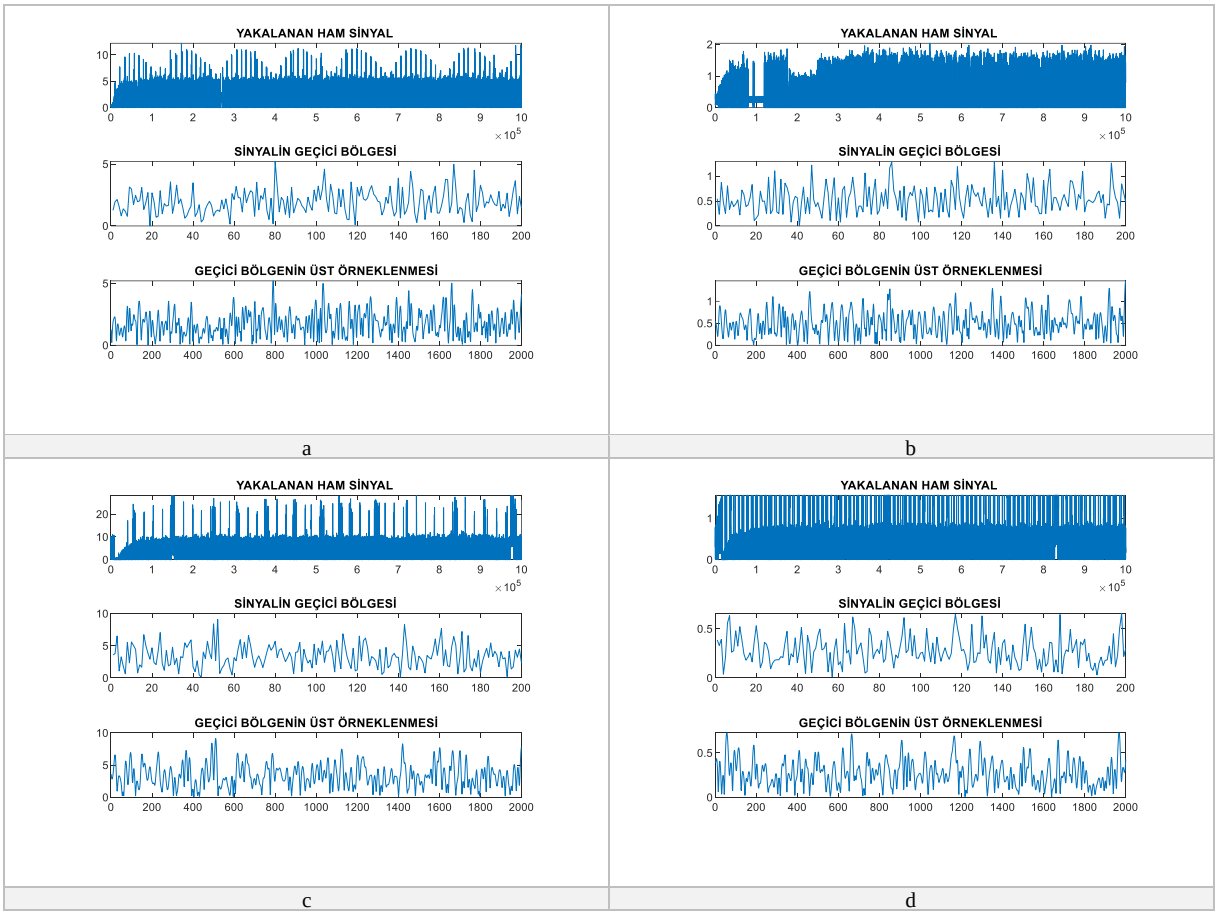
ve SNR'nin tanımlama doğruluğu incelenmektedir (Rehman, Sowerby, vd., 2014). (T.-Y. Lin vd., 2020), cihaz tanımlaması (DI) için RFF olarak PSD'yi kullanmıştır. Çok yollu kanal etkisi nedeniyle mesafe arttıkça tanımlama başarımı düşer. LTSP, alınan zaman etki alanı sinyalinden çıkarılır. PSD, Hızlı Fourier Dönüşümü'nden (FFT) sonra hesaplanır. CFO'lar, farklı girdilerin bir bileşimi kullanılarak da hesaplanabilir. Tablo 2.6'da IEEE standartlarında RF parmak izlerini belirleyen parametre ve sinyal bölümleri verilmektedir.

Tablo 2.6. IEEE 802 standartlarında parmak izi teknikleri

Referans	Standart	Sinyal bölümü	Parmak izi parametreleri	Hata oranı (%)
(Hall vd., 2004)	802.11	Geçici (transient)	Genlik, faz, güç, ayrık dalgacık dönüşümü	8
(Ureten ve Serinken, 2007)		Geçici (transient)	Genlik zarfı	12
(Suski II vd., 2008)		Öncül (preamble)	Güç tayf yoğunluğu	13
(Jana ve Kasera, 2008)		Veri (data)	Saat çarpıklığı	0
(Brik vd., 2008)		Veri (data)	Frekans hatası, senkronizasyon korelasyonu, I/Q ofseti, büyüklük ve faz hatası	0,34
(Danev ve Capkun, 2009)	802.15.4	Geçici (transient)	FFT tayfı	0,24

Kaynak: (Jana ve Kasera, 2008)

Şekil 2.15'te, oluşturduğumuz sinyal yakalama sistemiyle yakalanan ham RF sinyal örnekleri, bu sinyallerin geçici bölgesi ve öznitelik çıkarımı yaptığımız geçici bölgenin üst örneklemesi verilmektedir. RF sinyal örnekleri için şekil açıklamasında verilen sınıflara ait detaylı bilgiler Tablo 4.2'de verilmiştir.



Şekil 2.15. IoT cihazlardan yakalanan sinyal örnekleri (a - sınıf 11, b - sınıf 33, c - sınıf 55, d - sınıf 77)

2.5. RF Parmak İzi Veri Kümeleri

RF parmak izi veri kümeleri Wi-Fi, Bluetooth, LTE, ADS-B ve 5G v.d. kablosuz ağ teknolojilerini kullanan cihazlar vasıtasıyla oluşturulmaktadır. Ayrıca, Zigbee, NFC, RFID gibi diğer kısa menzilli kablosuz teknolojilerin parmak izleri de veri kümelerinde yer almaktadır. Her teknolojinin kendine özgü frekans tayfı, modülasyon türü ve veri biçimi olduğundan RF parmak izleri farklılık göstermektedir. Örneğin ADS-B, Automatic Dependent Surveillance-Broadcast (ADS-B) havacılık endüstrisinde kullanılan bir uydu navigasyon teknolojisidir. ADS-B parmak izleri, uydu frekansları, veri yapısı ve veri yayımlama frekansları gibi faktörlere dayanmaktadır.

RF parmak izi veri kümeleri aşağıdaki veri türleri kullanılarak oluşturulmaktadır.

- *Frekans spektrumları:* Wi-Fi, Bluetooth veya GSM sinyallerinin frekans spektrumlarının görselleştirilmesi.

- *Genlik verileri:* RF sinyal gücü ve yoğunluğu, genliği zaman içindeki değişimi veya istatistiksel özellikleri.
- *Modülasyon verileri:* Telefonun yaydığı Wi-Fi, Bluetooth veya GSM sinyallerinin modülasyon verileri.
- *Çoklu anten verileri:* Birden fazla anten tarafından ölçülen Wi-Fi, Bluetooth veya GSM sinyalleri ve gürültü verileri.
- *Zaman serisi verileri:* Wi-Fi, Bluetooth veya GSM sinyallerinin zaman serisi verileri.

Tablo 2.7'de literatür incelendiğinde RF parmak izi çalışmalarında kullanılan veri kümelerinin bir özeti verilmiştir.

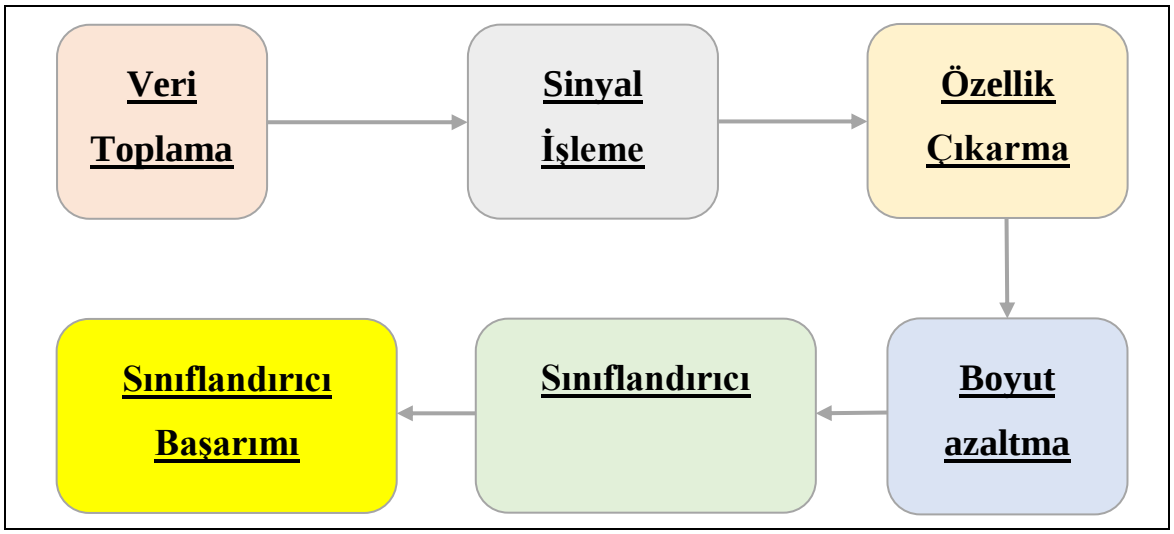
Tablo 2.7. RF parmak izi örnek veri kümeleri

Yapay/ Gerçek hayat	Frekans (GHz)	Dalga formu	Verici	Verici sayısı	Alıcı	Referans	Veri kümesi formatı
Gerçek hayat	2.4	Wi-Fi 2	IoT cihazlar, akıllı telefonlar	7	HackRF One	(Parmaksız ve Karakuzu, 2022b)	.mat/.csv
Gerçek hayat	2.4	Bluetooth	akıllı telefonlar	86	TDS7404 Tektronix	(Uzundurukan vd., 2020)	.txt
Gerçek hayat	2.4	out of standard	drone uzak denetleyicisi	17	MSOS604A Keysight	(Ezuma vd., 2020)	.mat
Gerçek hayat	1.09	ADS-B	uçak	100	BladeRF	(Liu vd., 2021)	.mat
Gerçek hayat	1.09	ADS-B	uçak	>140	B210 (USRP)	(Liu vd., 2020)	.mat
Yapay	2.45	Wi-Fi 2	X310	16	B210 (USRP)	(A. Jagannath vd., 2022)	SigMF
Yapay	2.4065	out of standard	M100 Dji	7	X310 (USRP)	(A. Jagannath vd., 2022)	SigMF
Yapay	2.685	Wi-Fi 2, LTE, 5G	X310	4	B210	(A. Jagannath vd., 2022)	SigMF
Yapay	2.432	Wi-Fi 2/3	X310, N210	20	N210 (USRP)	(Al-Shawabka, Restuccia, D'Oro, & Melodia, 2020)	SigMF

3. SİNYAL YAKALAMA VE VERİ TOPLAMA SİSTEMİ

Literatürdeki RF sinyal yakalama çalışmalarına ait özet Tablo 1.1 ve Tablo 1.2'de sunulmaktadır. Tablolardan da görüldüğü gibi sinyal yakalama süreçlerinde farklı alıcı ve vericiler kullanılmıştır. Bu bölümde, IoT cihazlarının RF parmak izini içeren çalışmalarda yaygın olarak kullanılan genel bir yapıyı (Şekil 3.1) takip eden çalışmamızda kullandığımız yöntemleri, teknikleri ve Şekil 3.1'de görsel olarak sunulan deney düzeneği açıklanacaktır.

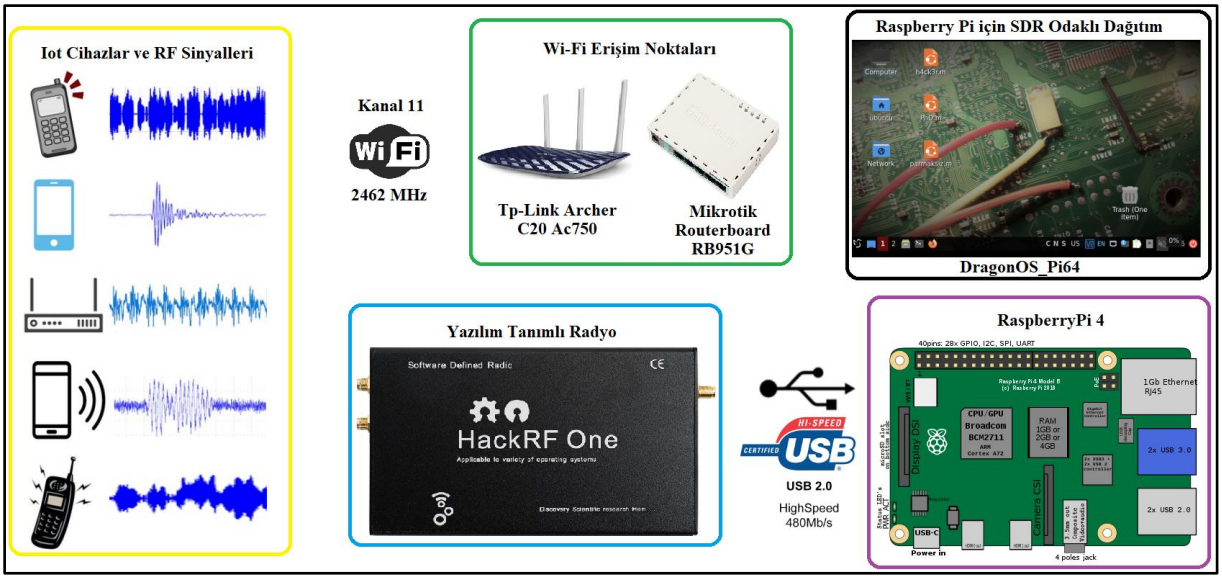
Şekil 3.1'de bu çalışmada takip edilen iş/işlem öbek yapısı verilmiştir. Şekilden de görüleceği üzere; ilk adım, RF sinyalini yakalamak ve analiz için işlemektir. Daha sonra işlenmiş sinyalden önceden belirlenmiş özellikleri çıkarmak ve bir sınıflandırıcıya göndermeden önce boyutlarını küçültmek gerekmektedir. Sınıflandırıcı, sinyale sahip cihazın yetkili olup olmadığını veya belirli bir sınıfa ait olup olmadığını belirlemek ana görevini üstlenir. Son olarak, sınıflandırıcının başarımı değerlendirilir. Bu tez çalışmasında kullanılan donanım, yazılım ve teknikler ilerleyen alt bölümlerde daha detaylı olarak verilmektedir.



Şekil 3.1. Çalışmada takip edilen iş/işlem öbek yapısı

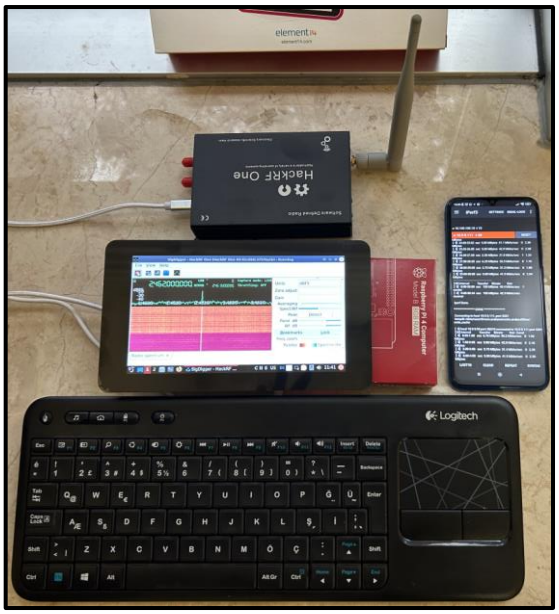
3.1. Veri Toplama Sistemi

IoT cihazlarından sinyal toplamak için, Şekil 3.2'de gösterildiği gibi bir sinyal toplama sistemi tasarlanmış ve gerçekleştirilmiştir. HackRF One SDR ile teleskopik antenler (ANT-DB1-LCD-ccc/ANT-LTE-WS-SMA/ANT500) kullanılmıştır. Hack RF One SDR, RF sinyal izleme ve yakalama için ve bir GNR yazılımı ile arayüzlenmiştir. Şekil 3.3, SigDigger programı kullanılarak RF sinyalinin kayıt aşamasında tezde kullanılan izleme sistemini göstermektedir.



Şekil 3.2. Geliştilen RF sinyal yakalama ortamı bileşenleri

Görevleri yürüten sanal makinenin, 2 soket ve 8 çekirdeği olan AMD EPYC 7502 işlemcisi ve 64 GB RAM'i bulunmaktadır. Sanal makinenin Windows işletim sistemi, açık kaynaklı bir sunucu sanallaştırma yönetim çözümü olan Proxmox Virtual Environment 7.2 üzerinde çalışır. QEMU/KVM ve LXC işletim sistemi, nesne tabanlı depolama altyapısı Ceph-Quincy Rados blok yapısı üzerine kuruludur. Matlab, toplanan ham sinyallerin geçici bölgelerini belirlemek, öznitelik çıkarma ve sınıflandırma işlemlerinde kullanılan algoritmaları ve yöntemleri yürütmek için kullanılır.

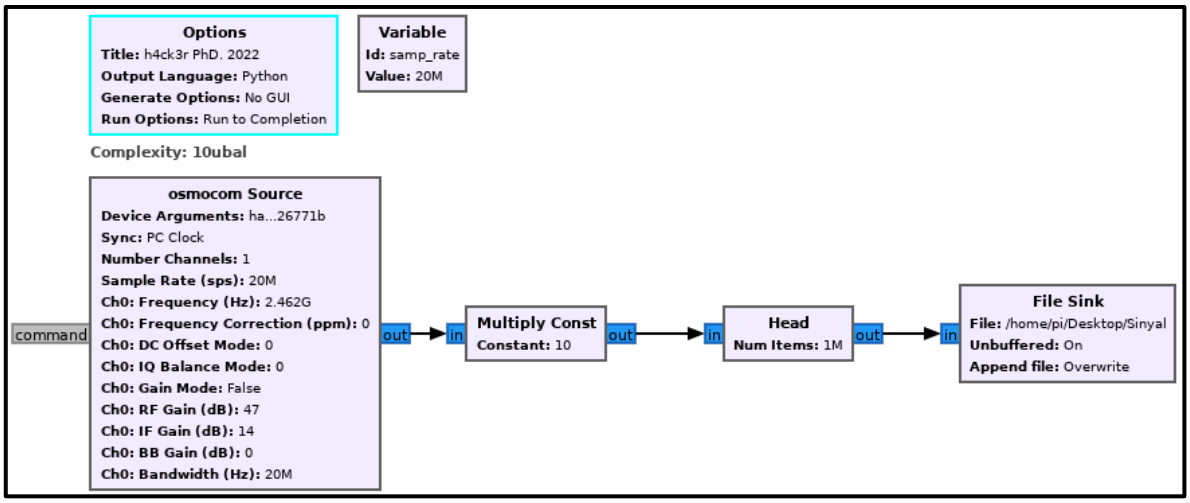


Şekil 3.3. HackRF One ve SigDigger programlarıyla oluşturulan sinyal izleme sistemi

Wi-Fi AP'ler, hem aktif hem de pasif modlarda çalışabilir; burada aktif mod, kablosuz cihazlara sürekli olarak sinyal göndererek ve veri aktarımını etkinleştirerek yüksek trafik durumlarında ağ başarımını iyileştirmek için kullanılır. Buna karşılık, pasif mod, erişim noktasının yalnızca diğer cihazlardan sinyal almasına izin verir ve bu cihazların kablosuz ağa bağlanmasına izin verir. Bu mod, enerji tasarrufunun öncelikli olduğu, trafiğin az olduğu ortamlar için kullanışlıdır.

DragonOS_Pi 64, SDR'lerle ilgilenen herkes için önceden yüklenmiş bir 22.04 aarch64 RPi işletim sistemidir. HackRF One, GNR ile çalışan bir SDR aksesuarıdır (Abirami vd., 2013). HackRF One, 1 MHz ila 6 GHz çalışma aralığı ve yazılım kontrollü anten bağlantı noktası gücü (3,3 V'ta 50 mA) ile saniyede 20 milyon örnekleme ile radyo sinyallerinin yarı çift yönlü iletimini sağlamak için tasarlanmış bir donanım ortamıdır.

GNU Radio, RF gerçek zamanlı uygulamalar için bir donanım aygıtının arka ucu olan sinyal işleme blokları sağlamaktadır. GNU Radio'daki programlar, grafiksel bir arayüz olarak, hem C++ hem de Python'da yazılır, derlenir ve işletim sistemlerine (örneğin DragonOS, Linux, Mac OSX ve Windows 10) sahip genel amaçlı işlemcilerin çoğunda çalıştırılmaktadır. Tipik olarak, GNU Radio'daki en yüksek programlama seviyesi Python'da yazılır (yani, sinyal işleme bileşeni başlatma ve kontrol) ve zamana duyarlı herhangi bir işlem C++'da yapılır. Şekil 3.4, bu çalışmada sinyal yakalama için GNU Radio yazılım paketinde kullanılan blokları ve bloklar aracılığıyla oluşturulan ilişkileri göstermektedir. Şekil 3.4'te verilen öbek şemada *kaynak bloğu (osmocom Source)*, örnekleme hızı tarafından tanımlanan sinyali yakalar veya alır ve belirtilen frekansla yükseltir. *Kaynak bloğu*, çeşitli donanım türlerini işleme, karmaşık veriler üzerinde çalışma ve tip I ve Q çıktı örnekleri üretme yeteneğine sahiptir. *Ana (Head) bloğu*, ilk N öğeyi çıkışa kopyalar ve ardından tamamlandı sinyali verir. Dosya havuzunu kullanırken, bir dosyaya kaç örneğin kaydedileceğini sınırlamak için çok kullanışlıdır. Akış grafiği seçenekleri "*GUI yok*" ve "*tamamlanana kadar çalıştır*" olarak ayarlanmışsa, ana bloğu, akış grafiğinde yalnızca bir dal olduğu sürece N örneğe ulaşıldığında akış grafiği yürütmesinin sona ermesine neden olur. Bir ikili dosyaya akış yazmak için Dosya Havuzu (File Sink) Bloğu kullanılır. Bu dosya, ikili dosyaları (MATLAB, C, Python, vb.) okuyabilen herhangi bir programlama ortamıyla uyumludur. Örneğin, karmaşık seçilirse ikili dosya, IQIQIQ sırasına göre float32'lerle doldurulacaktır. İkili veriler hiçbir meta veri veya başka bilgi içermemektedir.



Şekil 3.4. GNR programıyla sinyal yakalama işlemine ait öbek şema

Mikrotik ve Tp-Link AP'ler, Wi-Fi sinyallerini belirli kanallarda ve frekanslarda yayınlayabilir, 11. kanal ve 2462 MHz, sinyal aralığını sınırlamak için yaygın seçeneklerdir. Bu kanallar aracılığıyla iletişim kuran mobil cihazlardan veya Wi-Fi erişimi olan diğer cihazlardan gelen sinyalleri yakalamak ve izlemek için bir HackRF One cihazı kullanılır. HackRF One tarafından yakalanan sinyaller, DragonOS_Pi64 işletim sistemini çalıştıran bir RPi-4'te ve MEC'i etkinleştiren diğer bileşenleri işleyebilir. Sinyalleri yakalamak için, sinyali gönderen cihazlarda iperf3 istemci yazılımının kurulu olması, MEC cihazında ise iperf3 sunucu yazılımının kurulu olması ve TCP/5201 üzerinden gelen bağlantıları dinlemesi gerekir. Belirli bir ortam erişim kontrolü (MAC) adresine sahip bir cihaz, 5201 numaralı bağlantı noktası üzerinden MEC sistemine bağlandığında, sinyal yakalama ve kaydetme işlemini otomatikleştirmek için bir kabuk komut dosyası kullanılır. Mikrotik AP'lerdeki erişim kontrol listeleri (ACL'ler) de kontrol için kullanılır. MAC filtrelemenin etkinleştirildiği Tp-Link AP'leri aracılığıyla bağlanan istemciler için sinyal yakalama işlemi sırasında başka hiçbir erişim noktasının aynı frekanslarda yayın yapmadığından emin olmak önemlidir.

3.2. Sinyal Yakalama Çalışmalarında Kullanılan Donanım ve Yazılımlar

Açık kaynaklı yazılımlar (DragonOS, GNR v.d.) ve düşük maliyetli donanımlar (HackRF One, RPi-4) kullanılarak oluşturulan RF parmak izi yakalama sistemine ait işlem basamakları aşağıda verilmektedir:

- MEC olarak düşünülen mini bilgisayara (RPi-4 v.d.) sinyal yakalama sürecinde kullanılacak işletim sistemi (DragonOS, Raspbian v.d.) yüklenmektedir.

- Mini bilgisayar ile yazılım tanımlı radyo (HackRF One v.d.) gerekli sürücüler dahil birbirleriyle sorunsuz haberleştirilmektedir.
- Yazılım tanımlı radyo ile uyumlu sinyal işleme blokları sunan açık kaynak bir yazılım (GNR) kullanılmaktadır.
- Iot cihaz ile AP'nin 2.462 GHz frekansındaki haberleşme sinyali, HackRF One ve GNR yardımıyla yakalanarak kayıt altına alınmaktadır.
- GNR kullanarak sinyal filtrelenmekte ve demodüle edilmektedir.
- RF parmak izini oluşturmak için elde edilen ham sinyal, özellik çıkarma programının destekleyeceği formatta kaydedilmektedir.

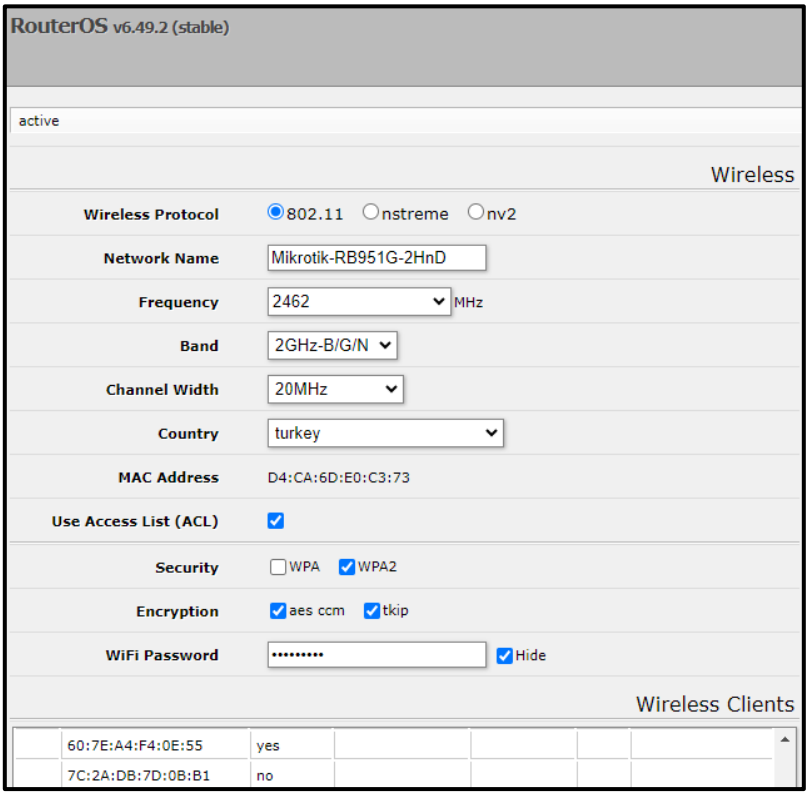
Tablo 3.1'de, RF sinyalleri yakalanırken kullanılan cihaz ve yazılımlar kullanım amaçları ile birlikte verilmektedir.

Tablo 3.1. RF sinyallerini yakalamak için kullanılan bileşenler

Kullanım amacı	Kullanılan cihazlar/yazılımlar
IoT cihazları	RPi4, RPi 400, Xiaomi Redmi Note 8, RPi3bp, Lenovo Tab M10, DN-7042-1
Kablosuz Erişim Noktaları	Tp-Link Archer C20 Ac750, Mikrotik RB951G-2HnD (Atheros AR9300)
Yazılım tanımlı radyo	HackRF One
HackRF One SDR ile uyumlu antenler	ANT-DB1-LCD-ccc/ANT-LTE-WS-SMA/ANT500
Yazılım radyolarını uygulamak için sinyal işleme blokları sağlayan ücretsiz ve açık kaynaklı yazılım geliştirme araç seti	GNU Radio
İşletim sistemleri	DragonOS Pi64, RPi OS 11
Kullanılan yazılımlar listesi	Matlab, Wireshark, Python, shell-script, Universal Radio Hacker (URH), SigDigger, RPi imager, SD Card Formatter, Win32 Disk imager, Git v.d.
Açık kaynak faydalı araçlar/komutlar	xxd, od, inspectrum, setxkbmap, nmcli, iwconfig v.d.

Ayrıca, sinyal gürültü oranının (SNR) yüksek olması RF parmak izi açısından avantaj sağlamaktadır. Sinyal yakalama işlemlerinde sinyal aralığını daraltmak amacıyla Şekil 3.5'de

ara yüzü verilen Mikrotik AP cihazı (Atheros AR9300 kablosuz) 2462 MHz frekansında yayın yapacak (kanal 11) şekilde yapılandırılmıştır.



Şekil 3.5. Mikrotik RouterOS v6.49.2 AP yapılandırması

Mobil kenar hesaplama için kullanılan RPi-4 mini bilgisayar üzerindeki kablosuz modülü aracılığıyla Şekil 3.6'da görüldüğü gibi Wi-Fi cihazlarının yayın yaptıkları kanal ve frekans bandlarına ulaşılabilmektedir. RPi ayrıca kendi Wi-Fi modülü haricinde USB Wi-Fi genişleticiler kullanılarak birden fazla Wi-Fi modülü *(wlan0-2)* olarak farklı bantlarda iletişim kurmayı sağlayabilmektedir.

```
pi@h4ck3r:~ $ sudo iwlist wlan0 channel | grep "2\."
          Channel 01 : 2.412 GHz
          Channel 02 : 2.417 GHz
          Channel 03 : 2.422 GHz
          Channel 04 : 2.427 GHz
          Channel 05 : 2.432 GHz
          Channel 06 : 2.437 GHz
          Channel 07 : 2.442 GHz
          Channel 08 : 2.447 GHz
          Channel 09 : 2.452 GHz
          Channel 10 : 2.457 GHz
          Channel 11 : 2.462 GHz
          Channel 12 : 2.467 GHz
          Channel 13 : 2.472 GHz
```

Şekil 3.6. Raspbian GNU/Linux 11 (bullseye) 2.4 GHz kanalların listelenmesi

RPi üzerinde bulunan kablosuz alıcı-vericinin üretici bilgilerine "*sudo lshw -C network | grep -B 1 -A 12 'Wireless interface'* " komutu ile ulaşılmaktadır. "*apt search lshw*" komutu ile *lshw* paketinin işletim sistemindeki görevi hakkında bilgi alınmaktadır. Şekil 3.7'de *lshw* komutu yardımıyla kablosuz arayüzler kolaylıkla listelenmektedir.

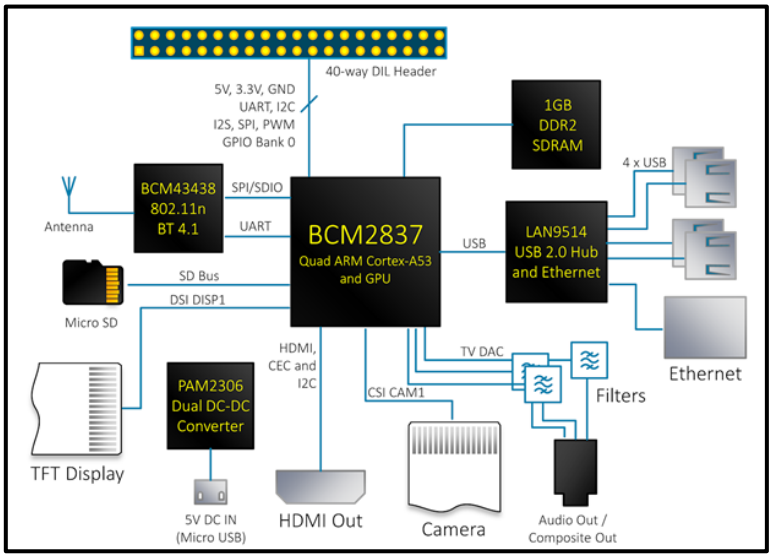
```
pi@h4ck3r:~ $ sudo lshw -C network | grep -B 1 -A 12 'Wireless interface'
  *-network:1
       description: Wireless interface
       physical id: 2
       logical name: wlan0
       serial: e4:5f:01:47:8c:15
       capabilities: ethernet physical wireless
       configuration: broadcast=yes driver=brcmfmac driverversion=7.45.241 fi
rmware=01-703fd60 multicast=yes wireless=IEEE 802.11
  *-network:2
       description: Wireless interface
       physical id: 3
       logical name: wlan1
       serial: d4:7b:b0:7e:a2:dc
       capabilities: ethernet physical wireless
       configuration: broadcast=yes driver=brcmfmac driverversion=6.10.198.66
 firmware=01-32bd010e multicast=yes wireless=IEEE 802.11
  *-network:3
       description: Wireless interface
       physical id: 4
       bus info: usb@1:1.1
       logical name: wlan2
       serial: 00:e0:4c:0b:b0:1e
       capabilities: ethernet physical wireless
       configuration: broadcast=yes driver=rtl8192cu driverversion=5.15.61-v7
l+ firmware=N/A link=no multicast=yes wireless=IEEE 802.11
```

Şekil 3.7. lshw komutu yardımıyla kablosuz arayüzlerin listelenmesi.

3.2.1. Mobil kenar hesaplama

Bu çalışmada, mobil kenar hesaplama kısmında mini bilgisayar RPi kullanılmaktadır. RPi-4 Model B, popüler RPi bilgisayar serisinin sonuncusudur. Önceki nesil RPi-3 Model B+

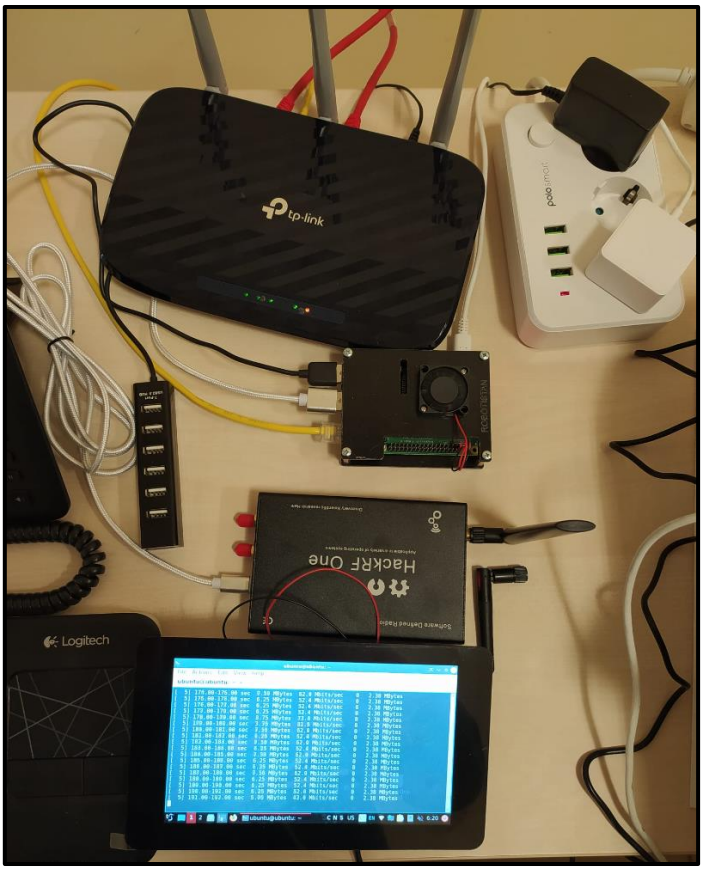
ile karşılaştırıldığında geriye dönük uyumluluğu ve benzer güç tüketimini korurken, işlemci hızı, multimedya performansı, bellek ve bağlantıda önemli artışlar sunar. RPi-4 Model B, giriş düzeyi x86 kişisel bilgisayar (PC) sistemleriyle karşılaştırılabilir masaüstü performansı sağlar (Süzen vd., 2020). RPi birçok işletim sistemini desteklemektedir. Sinyal yakalama süreçlerinde açık kaynaklı işletim sistemleri tercih edilmiştir. Bunun nedeni, açık kaynaklı sistemlerin kaynak gereksinimlerinin aşırı olmamasıdır. RPi yaygın olarak kendi donanımı ile uyumlu optimize çalışan RPi OS kullanmayı önermektedir. Şekil 3.8'de RPi-3 model B için donanım bileşenlerinin gösterildiği şema verilmiştir.



Şekil 3.8. RPi-3 mini bilgisayar bileşenleri şeması

Kaynak: (RPi-3 Block Diagram, 2023)

Tez kapsamında Bilimsel Araştırma Projeleri (BAP) ve bireysel olarak tedarik edilen cihazlar ile kurulan sinyal yakalama ve MEC kısmını içeren test ortamının ilk hali Şekil 3.9'da gösterilmektedir.



Şekil 3.9. Veri toplama sistemi (ilk hal)

Burada, Mikrotik üzerinden belirli kanallarda (örtüşmeyen kanal 11) ve frekanslarda (2462 Mhz) Wi-Fi yayını sağlanmaktadır. Mobil cihaz ya da Wi-Fi erişimi olan cihazlardan bu kanal ile iletişim esnasında araya HackRF SDR ile girilerek bu sinyallerin dinlenmesi ve yakalanması sağlanmaktadır. HackRF One ile yakalanan ya da izlenen sinyallerin MEC diye ifade edilen mobil kenar hesaplama süreçleri RPi üzerinde koşan DragonOS Pi_64 ve üzerindeki bileşenleri ile sağlanmaktadır.

3.2.2. İşletim sistemleri

RPi için, resmi olarak desteklenen işletim sistemi Raspberry Pi OS'dir. Debian tabanlı bu işletim sistemine ait mevcut güncel sürüm bilgileri aşağıda verilmektedir. Şekil 3.10'da komut satırı üzerinden "*lsb_release -a*" komutu ile işletim sistemine ait sürüm kontrolü yapılmaktadır.

```
pi@h4ck3r:~ $ lsb_release -a
No LSB modules are available.
Distributor ID: Raspbian
Description:    Raspbian GNU/Linux 11 (bullseye)
Release:        11
Codename:       bullseye
```

Şekil 3.10. Komut satırı üzerinden işletim sistemi sürümünün kontrol edilmesi

SD Card Formatter yazılımı ile işletim sistemi yüklenecek microSD kartın içeriğinin sıfırlama işlemi gerçekleştirilmektedir. Raspberry Pi Imager, RPi'nizle kullanıma hazır bir microSD karta işletim sistemi kurmamıza olanak sağlamaktadır. Tez çalışmalarında bu araç ile RPi OS ve sinyal analiz işlemleri için özelleştirilmiş DragonOS_Pi64 işletim sistemleri kurularak işlem yapılmıştır. "*setxkbmap -layout tr*" ile işletim sistemlerinde klavye katmanı *Türkçe* olarak ayarlanmaktadır.

DragonOS, SDR'ler için kullanıma hazır işletim sistemi olarak tasarlanmıştır. Bu işletim sisteminin geliştiricisi, Cema Xecuter'dır. Covid19 sürecinde durumu en iyi şekilde değerlendiren Cema Xecuter bunu fırsata çevirerek her zaman yapmak istediği bir şey olan RF hakkında daha fazla bilgi edinme şansını olumlu kullanmıştır. Ayrıca, Kali Linux'un saldırgan güvenlik, sızma testi, dijital adli tıp ve beyaz şapka korsanlığı üzerindeki muazzam olumlu etkisini görmüştür. Hedefi, Kali'den esinlerek en popüler ve erişilebilir SDR radyolarının çoğunu destekleyen, önceden yüklenmiş kapsamlı bir SDR yazılım araçları paketiyle bir Linux dağıtımı oluşturmaktır. DragonOS'un, Kali Linux'un saldırı güvenliği ve dijital adli tıp alanlarında tek durak noktası haline gelmesiyle aynı derecede SDR için başvurulacak kaynak olacağı düşünülmektedir.

DragonOS_Pi64, yazılım tanımlı radyolarla ilgilenen herkes için kullanıma hazır 22.04 aarch64 RPi tabanlı bir işletim sistemidir. DragonOS_Pi64'te yüklenen tüm yazılımlar /usr/src dizininde bulunurken, kalan yazılımlar paket yöneticileri tarafından yüklenir. HackRF One, RTL-SDR, LimeSDR, Ettus/USRP ve BladeRF gibi literatürde yaygın kullanılan SDR'ların kullanımına olanak sağlar. SigDigger, Universal Radio Hacker, GNU Radio, SDR++, Aircrack-NG, Kismet, GQRX, Wireshark, inspectrum, CubicSDR, v.d. yazılımları da işletim sistemine dâhil etmiştir (SourceForge, 2023).

3.2.3. Yazılım tanımlı radyo

SDR, telsiz iletişimi için bir teknolojidir. Bu teknoloji, donanım tabanlı çözümlerin aksine, yazılım tanımlı kablosuz protokollere dayanmaktadır. Bu, üzerinde uygulandıkları donanımı değiştirmeye gerek kalmadan yeniden programlama yoluyla güncelleme ve yükseltme gibi çeşitli özelliklerin ve işlevlerin desteklenmesi anlamına gelir ve çok bantlı ve çok işlevli kablosuz cihazları gerçekleştirme olasılığının kapısını açar (Akeela ve Dezfouli, 2018). Kablosuz İnovasyon Forumu, SDR'yi *"fiziksel katmanın bazı veya tüm işlevlerinin yazılım tarafından gömüldüğü radyo"* olarak tanımlamıştır. SDR, donanım iletişim cihazlarının geleneksel uygulamalarının yerine yeniden yapılandırılabilir kablosuz iletişim sistemi geliştiren devrim niteliğinde bir yaklaşım olarak ortaya çıkmıştır (Gummineni ve Polipalli, 2020). Küçük tasarım değişiklikleri ile donanımı yükseltmek için herhangi bir zamanda yeni bir devre kurmak çok zor olacaktır (Miyashiro vd., 2017). SDR, aynı donanım platformunun farklı protokollere sahip birçok terminal için yeniden kullanılmasına izin vererek pazara sunma süresini ve geliştirme maliyetini azaltır (Sruthi vd., 2013). Bir raporda (Akeela ve Dezfouli, 2018), SDR pazarının 2021 yılına kadar 29 milyar doları aşacağı tahmin edilmektedir. Global Industry Analysts, Inc., SDR için bazı pazar eğilimlerini şu şekilde vurgulamaktadır: (i) artan ilgi askeri sektörden gelişmekte olan ülkelerde iletişim sistemleri kurma ve geniş ölçekli dağıtım, (ii) kamu güvenliği ve afete hazırlık uygulamalarına yönelik artan talep ve (iii) sanallaştırılmış baz istasyonları (BS'ler) oluşturma. SDR'ler ayrıca geleceğin uzay iletişimini geliştirmek için de idealdir (Paillassa ve Morlet, 2003), (Angeletti vd., 2014), Küresel Navigasyon Uydu Sistemi (GNSS) sensörleri (Seo vd., 2011), Araçtan -Araca (V2V) iletişim (Xiong vd., 2015), (Tiwari vd., 2014), (Kloc vd., 2017) ve IoT uygulamaları (Zhou vd., 2016), (J.-S. Park vd., 2016) nispeten küçük ve düşük güçlü SDR'lerin kullanılabileceği yerlerden bazılarıdır. ANT500 teleskopik antenle donatılmış bir HackRF One SDR, sinyal kaydı için yaygın olarak kullanılır ve bir GNU Radyo uygulaması aracılığıyla arabirim oluşturulabilir. HackRF One, 20 Mbps'ye kadar sinyalleri örnekleyebilen ve 8 bit ADC çözünürlüğüne sahip nispeten ucuz bir SDR'dir (Samuel, 2018).

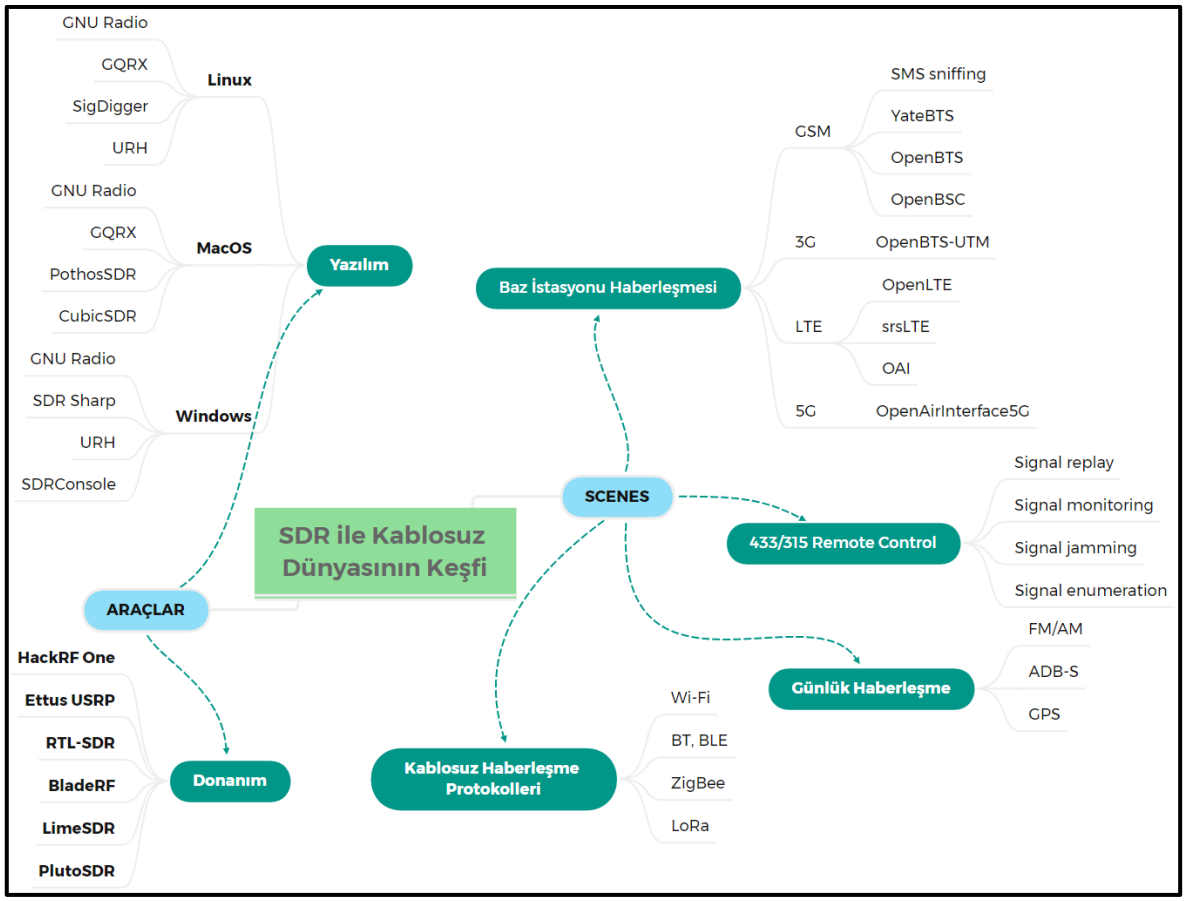
Tablo 3.2'de yaygın olarak kullanılan yazılım tanımlı radyolar karşılaştırılmaktadır. Wi-Fi RF parmak izi için SDR'ların yanı sıra Rohde & Schwarz FSH8, Tektronix RSA5000, Anritsu MS2700C, Agilent N9310A ve Keysight Teknolojileri UXR gibi tayf analizörleri de kullanılmaktadır.

Tablo 3.2. Yazılım tanımlı radyoların karşılaştırılması

	HackRF	RTL-SDR	LimeSDR	BladeRF		USRP		
				x40	x115	B100	B200	B210
Radyo spektrumu	30 MHz – 6 GHz	22 MHz – 2.2 GHz	100 KHz – 3.8 GHz	300 MHz – 3.8 GHz		30MHz–2.2GHz	50 MHz – 6 GHz	
Bant genişliği	20 MHz	3.2 MHz	61.44 MHz	28 MHz		16MHz	61.44 MHz	
Dupleks	Yarım	U/D	Tam	Tam		Tam	2x2 MIMO	
Örnekleme boyutu	8 bit	8 bit	12 bit	12 bit		12/14 bit	12 bit	
Örnekleme oranı	20 Msps	3.2 Msps	61.44 Msps	40 Msps		64/128 Msps	61.44 Msps	
Arayüz (hız)	USB 2 (480 megabit)	USB 2 (480 megabit)	USB 3 (5 gigabit)	USB 3 (5 gigabit)		USB 2 (480 megabit)	USB 3 (5 gigabit)	
Mikrodenetleyici	LPC43XX	ESP32 CC1101	Cypress FX3 CYUSB3014	Cypress FX3		Cypress FX2	Cypress FX3	
RF alıcı-verici	MAX5864, MAX2837, RFFC5072	RTL2832U	LMS7002M	LMS6002M LMS6002D		AD9364	AD9361	
Açık kaynak	Evet	Hayır	Evet	HDL + Code schematics		HDL + Code schematics	Host Code	
Fiyat	~320$	~40$	~350$	~420$	~650$	~675$	675$	~1100$

Kaynak: (Akhtyamov vd., 2015)

Şekil 3.11'de bir SDR ile kablosuz haberleşen cihazların etkileşimi görülmektedir. *Donanım* kısmında, literatürde kullanılan SDR çeşitliliği verilmektedir. *Yazılım* kısmında, SDR'ların kullanıldığı işletim sistemi ve işletim sistemleri üzerinde koşan sinyal işleme programları verilmektedir. *Sahneler (Scenes)* kısmında ise Wi-Fi iletişim protokolleri ve uygulama alanları verilmektedir.



Şekil 3.11. Yazılım tanımlı radyo ile kablosuz haberleşme keşfi

SDR ve/veya spektrum analizörü seçimi yapılırken dikkat edilecek kısımlar aşağıda verilmektedir:

- *Frekans aralığı:* SDR veya spektrum analizörü, çoğu Wi-Fi ağı tarafından kullanılan bantlar olan 2,4 GHz ve 5 GHz bantlarını alıp iletebilmelidir.
- *Hassasiyet:* SDR veya spektrum analizörü, zayıf Wi-Fi sinyallerini alacak kadar hassas olmalıdır.
- *Bant Genişliği:* Wi-Fi sinyalinin tamamını yakalamak için SDR veya spektrum analizörü geniş bir bant genişliğine sahip olmalıdır.

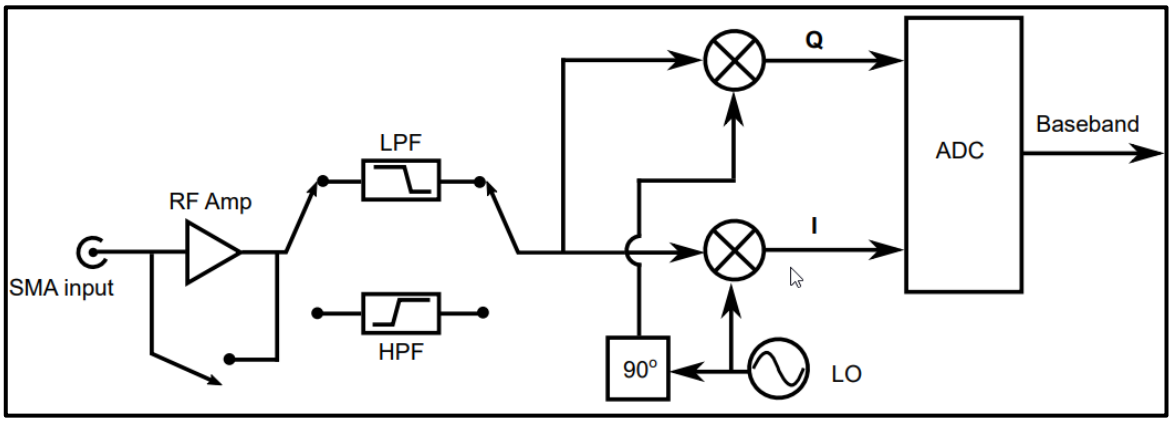
- *Maliyet:* SDR'ler ve spektrum analizörlerinin fiyatları birkaç yüz dolardan on binlerce dolara kadar değişebilir. Bütçenize uygun bir SDR veya spektrum analizörü seçmeniz önemlidir.

Tez kapsamında kullanılan yazılım tanımlı radyo Şekil 3.12'de verilmektedir. HackRF One radyo sinyallerini iletebilen veya alabilen güncel donanım platformudur. Yeni nesil radyo teknolojilerinin test edilmesini ve geliştirilmesini sağlamak için tasarlanan HackRF One, USB çevre birimi olarak kullanılabilen veya bağımsız çalışma için programlanan açık kaynaklı bir donanım platformudur. SDR yazılım tabanlı dijital ses teknikleri benzeri dijital sinyal işlemenin radyo dalga formlarına uygulanmasıdır. Tıpkı bir bilgisayardaki ses kartı ile ses dalgaları sayısal hale getirildiği gibi, HackRF çevresel yazılım da radyo dalgalarını sayısal hale getirir. Hoparlör ve mikrofonun yerine anten kullanılabilmektedir. Akademik çalışmalarda HackRF One üreticisi ANT500 teleskopik anten kullanımını önermektedir.

Şekil 3.12. HackRF One yazılım tanımlı radyo

Şekil 3.13 HackRF One'ın alıcı tarafının bir blok diyagramını göstermektedir. Antenden (SMA konektörü) gelen RF giriş sinyali, sinyalin aktif cihaz aracılığıyla atlanabildiği, kullanıcı tarafından değiştirilebilen bir geniş bant *düşük gürültülü yükseltici (low noise amplifier),* 14 dB kazanç, MGA-81563 ile yükseltilmektedir. Seçilen frekans aralığına bağlı olarak bir *yüksek geçiren filtre (HPF)* veya *alçak geçiren filtre (LPF)* ile filtrelenebilmektedir. Dörtlü

karıştırıcısı, faz içi (I) ve kareleme (Q) olarak adlandırılan iki bileşen sunmaktadır. Lokal Osilatör sinyali, doğrusal olmayan bir bileşen üzerinde hareket ettiğinde, yüksek frekanslı giriş bandını IF aralığına getirmektedir. Voltaj kontrollü osilatör, RFFC5072 yonga seti ile faz kilitli döngü stabilize karıştırıcı, gelen frekans enerjisini 2.3 GHz ile 2.7 GHz arasında bir IF'ye çevirir, daha sonra 8 bitlik analogdan dijitale dönüştürücü (ADC) ile sayısallaştırılmaktadır. Özellikle HackRF One, bandı bir kerede 22 MHz'e kadar kapsayan bir ADC'ye, MAX 5864'e sahiptir. Maksimum SDR, 20 MHz'lik bir bant genişliğine ayarlanmıştır ve akışı daha sonra 32-bit ARM Cortex işlemcisine, LPC43XX'e gönderilir, daha sonra USB kanalına aktarılmaktadır. RTL birimlerinin IF'leri 3.57 MHz veya 4.57 MHz (R802 tuner durumunda) veya hatta sıfır IF (feshedilmiş E4000 tuner) aralığındadır. Düşük bir IF seçimi daha iyi seçicilik sağlarken, daha yüksek IF'ler daha düşük mikser görüntü yanıtları ile sonuçlanır, bu nedenle seçicilik ve görüntü yanıtı arasında bir değiş tokuş vardır (Valkanas v.d., 2019).



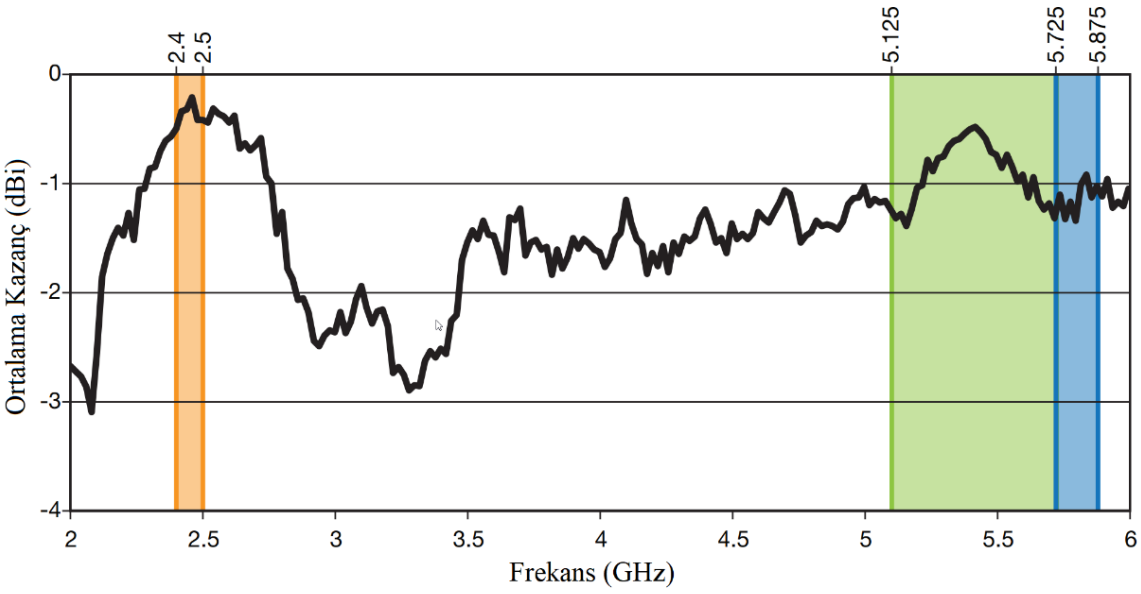
Şekil 3.13. HackRF One alıcı tarafı öbek şeması

Kaynak: (Perotoni ve dos Santos, 2021)

3.2.4. Anten seçimi

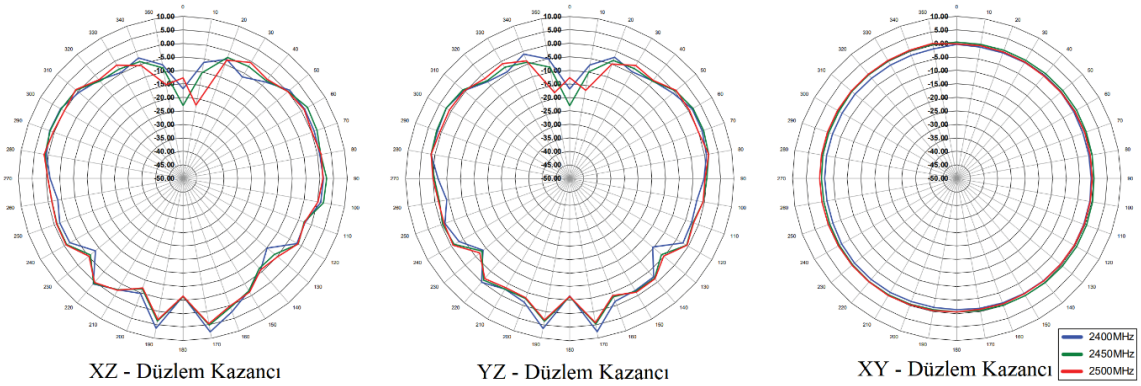
Sinyal yakalama aşamalarında HackRF cihazı ile ANT-DB1-LCD-ccc anten kullanılmıştır. Bu antenin ortalama kazanç değerleri Şekil 3.14'te, düzlem kazanç değerleri ise Şekil 3.15'de verilmiştir. Sinyal tayf izleme aşamalarında, HackRF cihazı ile ANT-LTE-WS-SMA anten kullanılmıştır. Genellikle bir antenin kazancı, antenin belirli bir yöne yönlendirebileceği güç miktarını tanımlayan bir ölçü birimi olan dBi (desibel-izotropik) cinsinden ölçülür. Daha yüksek bir dBi değeri, daha yüksek bir kazancı ve sinyali belirli bir yöne yönlendirmek için daha güçlü bir yeteneği gösterir.

Anten kazancı, bir antenin bir radyo sinyali iletilirken veya alınırken sağladığı güç artışını ifade eder. Genellikle desibel (dB) cinsinden ölçülür ve antenin girişindeki bir sinyalin güç seviyesinin antenin çıkışındaki aynı sinyalin güç seviyesine oranıdır.



Şekil 3.14. ANT-DB1-LCD-ccc anteninin ortalama kazanç değerleri

Kaynak: (Tme Eu, 2023)



Şekil 3.15. ANT-DB1-LCD-ccc anteninin düzlem kazanç değerleri

Kaynak: (Tme Eu, 2023)

Bir antenin kazancı, tasarımı ve şekli ile çalıştığı frekanstan etkilenir. Bir antenin kazancı iki şekilde açıklanabilir:

- *İzotropik kazanç:* Bu, her yöne eşit olarak yayıldığı varsayıldığında, bir antenin teorik maksimum kazancıdır. Genellikle farklı antenlerin kazancını karşılaştırmak için bir referans noktası olarak kullanılır.

- *Direktif kazancı:* Bu, yayıldığı yön dikkate alındığında, bir antenin gerçek kazancıdır. Genellikle dBi (izotropik bir radyatöre göre desibel) cinsinden ölçülür. Örneğin bir çift kutuplu anten, merkez frekansında 2,15 dBi'lik bir kazanca sahiptir, bu da bir sinyale izotropik bir antenden 2,15 dB daha fazla güç sağladığı anlamına gelir. Örneğin bir yama anteninin 9dBi kazancı vardır, bu da bir sinyale izotropik bir antenden 9 dB daha fazla güç sağladığı anlamına gelir. Daha yüksek kazancın her zaman daha iyi performans anlamına gelmediğini belirtmekte fayda var. Daha yüksek kazançlı antenler daha yönlü olabilir ve belirli durumlarda iyi performans göstermeyebilir.

VSWR (Voltage Daimi Dalga Oranı), anten ile iletim hattı arasındaki uyumun kalitesinin bir ölçüsüdür. İletim hattında meydana gelebilecek duran dalganın maksimum genliğinin (veya "geriliminin") minimuma oranıdır. 1:1'lik bir VSWR, anten ile iletim hattı arasında mükemmel bir eşleşme olduğunu gösterir ve tüm RF enerjisinin antene iletildiği anlamına gelir. VSWR ne kadar yüksek olursa, RF enerjisinin yansıması o kadar büyük ve gerçekte antene iletilen enerji miktarı o kadar düşük olur. 2:1'lik bir VSWR, antene iletilen her 2 birim enerji için 1 birim enerjinin geri yansıtıldığı anlamına gelir. 3:1'lik bir VSWR, antene iletilen her 3 birim enerji için 1 birim enerjinin geri yansıtıldığı anlamına gelir. Daha düşük VSWR, antenin iletim hattıyla daha iyi eşleştiği ve antene daha fazla RF enerjisinin iletildiği anlamına gelir. Aşağıda 2,4 GHz'de yaygın WiFi anten türleri verilmektedir:

- *Çok yönlü antenler:* Bu antenler, sinyalleri her yöne yayarak 360 derecelik bir yarıçapta kapsama alanı için idealdir. Yönlendiriciler ve erişim noktaları gibi cihazlarda yaygın olarak kullanılırlar.
- *Yönlü antenler:* Bu antenler, sinyalleri belirli bir yönde yayacak şekilde tasarlanmıştır ve bu bir sinyalin iletilebileceği mesafeyi artırabilir. Genellikle noktadan noktaya ve noktadan çok noktaya uygulamalarda kullanılırlar.
- *Panel antenler:* Bu antenler tipik olarak düz ve dikdörtgen şeklindedir ve genellikle geniş açılı bir radyasyon modelinin gerekli olduğu ancak düşük bir profilin istendiği durumlarda kullanılır.
- *Yagi antenleri:* Bu antenler tipik olarak uzun menzilli, yönlü bir sinyalin gerekli olduğu durumlarda kullanılır. Genellikle noktadan noktaya ve noktadan çok noktaya uygulamalarda kullanılırlar ve sinyali belirli bir yöne odaklamak için birlikte çalışan birden çok öğeden oluşurlar.

3.2.5. Açık kaynak sinyal yakalama yazılımları

Sinyal yakalama ve izleme çalışmalarında, GNU Radio, SigDigger ve Universal Radio Hacker olmak üzere açık kaynaklı üç yazılım öncülük etmektedir. Tezin deneysel çalışmalar safhasında GNR ile oluşturulan ilk sinyal yakalama ve kayıt modeli Şekil 3.18'de verilmektedir.

3.2.5.1. GNU Radio

Ücretsiz sayısal sinyal işleme platformu *GNU Radio* 3.9 güncel sürümü ile isteğe bağlı radyo sistemleri, modülasyon şemaları oluşturmanıza izin veren bir dizi program ve kitaplık içermektedir. Alınan ve gönderilen sinyallerin şekli yazılımda konfigüre edilmektedir, sinyalleri yakalamak ve üretmek için basit donanım cihazları kullanılmaktadır.

Yazılım, frekans bandına ve sinyal modülasyonu türüne bağlı olmayan evrensel programlanabilir alıcı-vericilerle birlikte, GSM ağları için baz istasyonları, RFID etiketlerinin uzaktan okunması için cihazlar (elektronik tanımlamalar ve geçişler, akıllı kartlar), GPS alıcıları, Wi-Fi, FM radyo alıcıları ve vericileri, TV kod çözücüleri, pasif radarlar, spektrum analizörleri vb. cihazlar oluşturmak için kullanılabilmektedir.

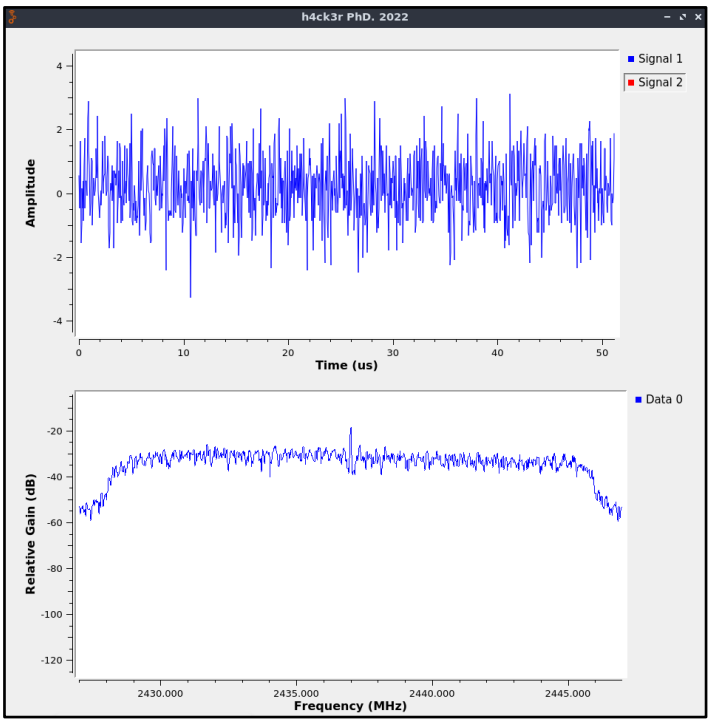
Ayrıca USRP'ye ek olarak, sinyal girişi ve çıkışı için diğer donanım bileşenlerini kullanabilmektedir. Örneğin, ses kartları, TV alıcıları, BladeRF, Myriad-RF, HackRF, UmTRX, Softrock, Comedi, Funcube, FMCOMMS, USRP ve S-Mini cihazları için sürücüleri mevcuttur.

SDR (Software Defined Radio) sistemlerinde, birçok radyo alıcısı ve vericisi, RF sinyallerinin çift taraflı darbe genişliği (IQ) sinyallerini kullanmaktadır. IQ sinyali, birbirine dik iki ayrı parçadan (In-phase (I) ve Quadrature-phase (Q)) oluşmaktadır. Orijinal RF sinyalini elde etmek için bu iki sinyal birbirleriyle çarpılmaktadır. Bu karmaşık sinyal, sinyalin gerçek değeri ve sanal bileşenini içerdiğinden sinyal işleme sürecini tetiklemektedir. GNU Radio'da *Complex to Mag* bloğu, kompleks veri akışını gerçek sayısal veri akışına dönüştürerek gerçek sayısal işlemeye hazır hale getirmektedir.

Şekil 3.4'teki diyagram https://github.com/HuseyinPARMAKSIZ/RF-Fingerprint-Data-Acquisition" adresinde "izle.grc" isimli dosya olarak verilmiştir. Aynı dizin altında çalıştırılabilir "izle.py" isimli Python dosyası verilmektedir. GNU Radio'da düzenlenen öbek şema ile sinyal kayıt süreci için bu Python dosyası yürütülmektedir. Python dosyası

işletildiğinde eş-zamanlı olarak QT GUI Frequency ve Time Sink arayüzleri ile kayıt altına alınan sinyal incelenebilmektedir..

Şekil 3.16'de örnek bir akıllı telefonun speedtest/iperf3 testleri anında kayıt altına alınan sinyalin temsili bir bölümü verilmektedir.



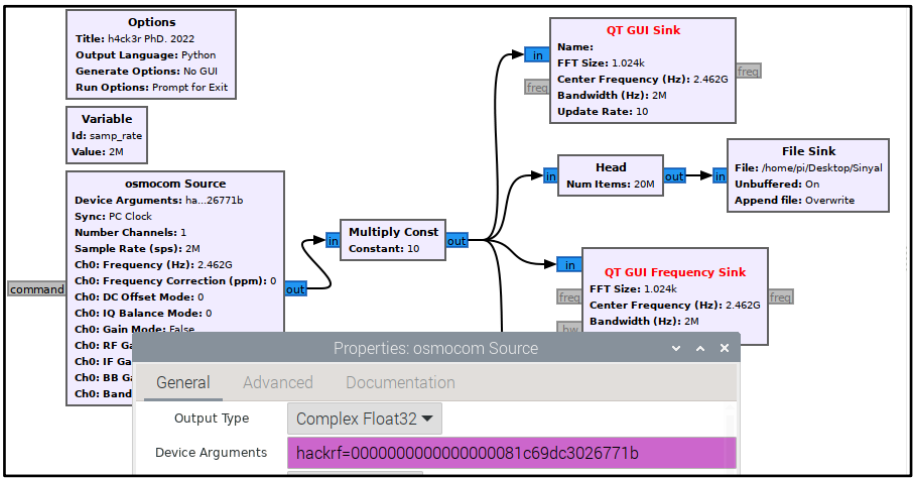
Şekil 3.16. GNR'de RF sinyalinin kontrolü (genlik (üst), bağıl kazanç (alt))

Raspbian işletim sisteminin deposunda varsayılan olarak gelen GNR sürümünün tespiti için "*apt search gnuradio-companion*" komutu kullanılmaktadır. Apt (Advanced Package Tool), Debian tabanlı dağıtımlarda paket yönetimi için kullanılan bir komut satırı aracıdır. Apt, Ubuntu'nun yazılım depolarından paketleri indirmek, yüklemek, kaldırmak, güncellemek ve yapılandırmak için kullanılmaktadır. Ayrıca işletim sisteminde GNR'nin olup olmadığı "dpkg-query –l | grep 'GNU Radio Sofware' " komutuyla öğrenilmektedir.

HackRF One SDR cihazı için bağlı olduğu işletim sistemi komut satırında *hackrf_info* komutu ile cihaza ait detaylı bilgilere Şekil 3.17 kod kümesi ile ulaşılabilir. Uygulamalarda birden fazla SDR cihazı kullanılması durumları olabilir. Bu durumda GNU Radio uygulamasında *source* olarak eklenen diyagramın "*Device Arguments*" parametresi (*hackrf=serial number*) Şekil 3.18 gibi düzenlenlenmelidir.

```
pi@h4ck3r:~/Desktop $ hackrf_info
hackrf_info version: unknown
libhackrf version: unknown (0.5)
Found HackRF
Index: 0
Serial number: 000000000000000081c69dc3026771b
Board ID Number: 2 (HackRF One)
Firmware Version: 2021.03.1 (API:1.04)
Part ID Number: 0xa000cb3c 0x00584766
```

Şekil 3.17. HackRF One SDR bilgilerinin gösterimi

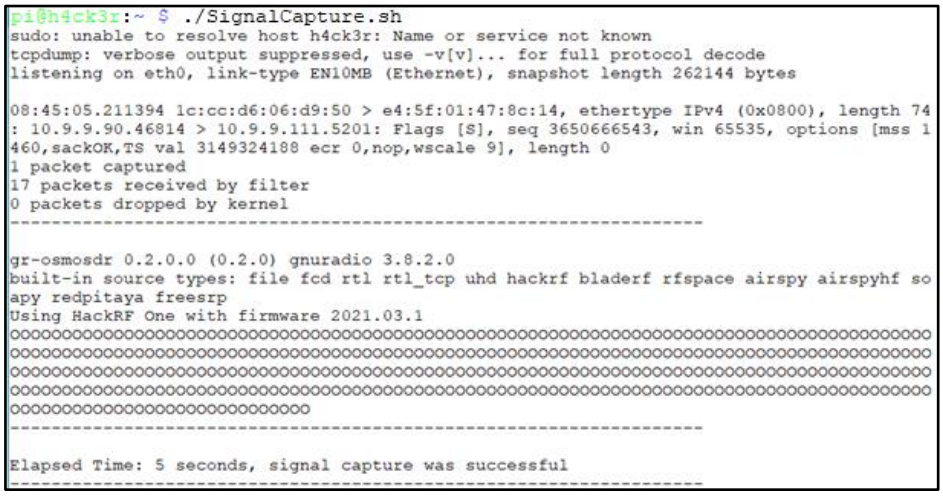


Şekil 3.18. GNR'de kullanılacak SDR kaynağının belirlenmesi

lsusb | grep HackRF komutu çıktısı: Bus 001 Device 003: ID 1d50:6089 OpenMoko, Inc. Great Scott Gadgets HackRF One SDR şeklindedir. Burada, 1d50 üretici (OpenMoko, Inc.) için ID numarasıdır. 6089 ise aygıt (Great Scott Gadgets HackRF One SDR) detaylarını belirleyen ID numarasıdır.

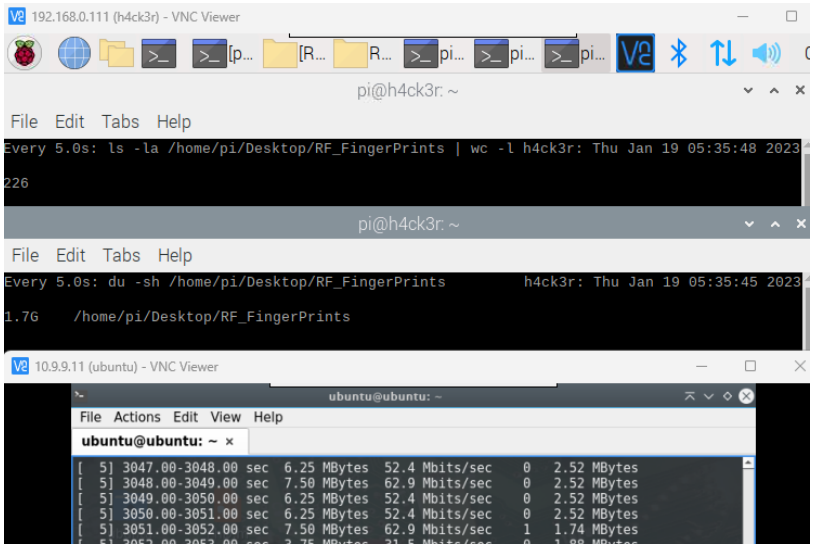
GNR aracılığıyla sinyal yakalama ve kaydetme süreçlerini otomatize etmek için yazılan kabuk betiği https://github.com/HuseyinPARMAKSIZ/RF-Fingerprint-Data-Acquisition" adresinde "SignalCapture.sh" isimli dosya olarak verilmiştir. Bu betik aracılığıyla RF sinyal üzerinde belirli işaretler oluşturulmaktadır. Sinyalin ön-işleme kısımlarında bu işaretler önemli rol almaktadır. Bu betikle ayrıca kayıt altına alınan sinyale zaman damgası verilmektedir. *od -f -w8 Sinyal.2022.04.05-17.33.41 > IQ.Sinyal.2022.04.05-17.33.41.txt* ile belirli zamanda kayıt altına alınan sinyalin I/Q formatında bileşenlerini farklı bir dosyada kayıt altına almak mümkün olmaktadır. Kayıt altına alınan ham sinyallerin tayf incelemesi "*inspectrum -r 20e6 Sinyal.2022.04.18-09.41.33"* komutu ile yapılabilmektedir. Ayrıca URH ile kayıt altına alınan

RF sinyalinin hem açık kaynaklı işletim sistemleri hem de Windows işletim sistemlerinde analizi yapılabilmektedir.



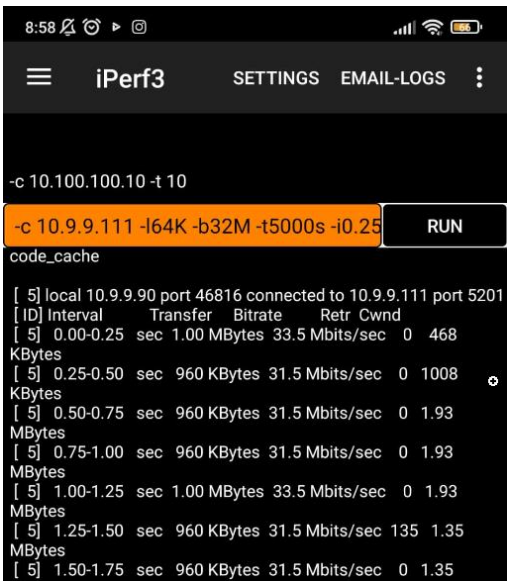
Şekil 3.19. RF sinyal kayıt betiği çalışma sonuç ekran görüntüsü

Şekil 3.19'da sinyal yakalama betiği çalıştırıldıktan sonra yaklaşık 5sn'de bir sinyal örneği kayıt altına alınmaktadır. Sinyal kayıtlarını saydırmak için Linux/Unix sisteminde komut satırında belirli bir komutu sürekli olarak çalıştırmak ve sonuçları düzenli aralıklarla güncellemek için kullanılan "watch" aracı kullanılmaktadır. RPi-4 üzerinde çalışan süreçlerin takip edilebilmesi için ekran maliyetinden kaçınılması gereken durumlarda VNC, RDP gibi uzak masaüstü yardımcı servisleri kullanılmaktadır. Şekil 3.20'de hem iperf testi yapan istemci hemde iperf yapılan sunucuya ait çalışan süreçlerin verildiği VNC viewer arayüzü bulunmaktadır.

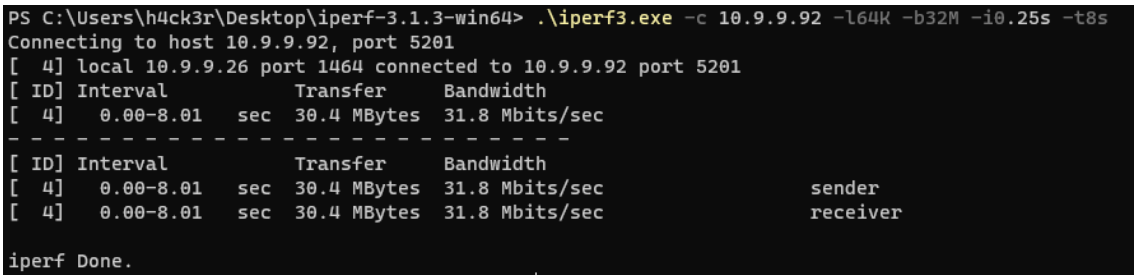


Şekil 3.20. VNC ile RPi-4 üzerindeki süreçlerin uzaktan izlenmesi

iperf testlerinde istemci mobil bir cihaz ise Şekil 3.21'deki gibi "Aruba Utilities v.b." yazılımlar kullanılabilir. Eğer istemci tarafı Windows, Linux v.d. işletim sistemleri ise iperf'ün güncel sürümü olan iperf3 paketi kullanılmaktadır. Şekil 3.22'de Windows işletim sisteminde yapılan iperf3 örneği verilmektedir.



Şekil 3.21. Mobil cihazlarda Aruba Utilities programı ile iperf uygulanması



Şekil 3.22. Windows'ta iperf3 bantgenişliği testi sonuç ekranı

3.2.5.2. SigDigger

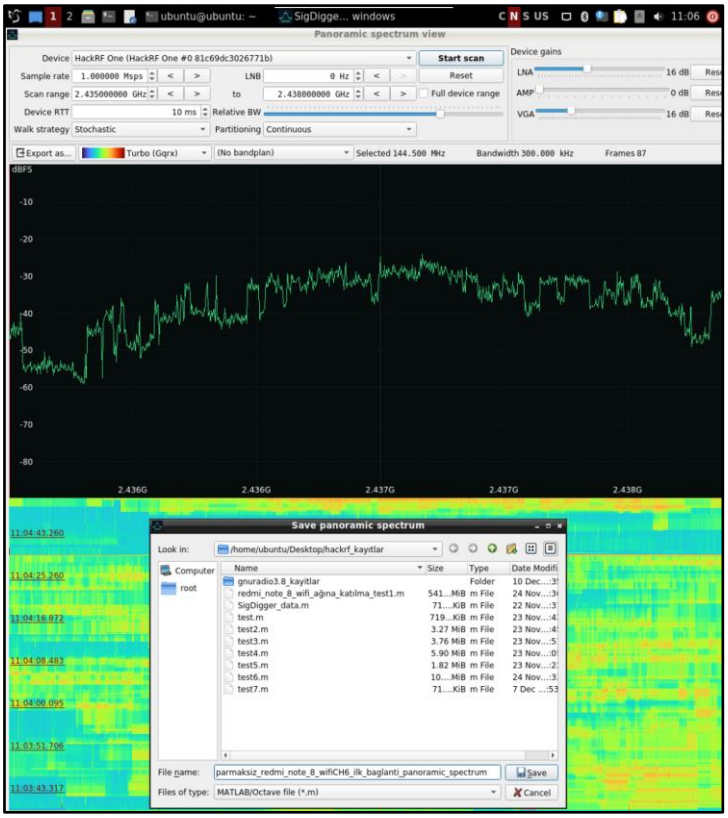
SigDigger, bir sinyal kayıt ve analiz aracıdır. Bu program, sıralı bir veri dosyasını (örneğin, HackRF One veya RTL-SDR tarafından kaydedilen sinyal) okuyarak ve bu veriyi grafiklerle görüntüleyerek sinyal içindeki bilgiyi incelemenizi sağlar. RF parmak izi çalışmalarında, SigDigger kullanılarak elde edilen sinyallerin analizi yapılabilir ve RF parmak izi için gerekli özellikler çıkarılabilir. SigDigger, bilinmeyen radyo sinyallerinin bilgilerini çıkarmak için tasarlanmış, GNU/Linux veya MacOS gibi Unix sistemleri için BatchDrake'in Qt5'te yazdığı bir grafik, dijital sinyal analizörüdür. Mevcut alternatiflerin aksine SigDigger, GNU Radio'ya dayalı değildir. Bunun yerine, yükü dağıtmak için çok çekirdekli CPU'ları

kullanan kendi DSP kitaplığını (sigutils) ve gerçek zamanlı bir sinyal analiz kitaplığını (Suscan) kullanmaktadır. Ayrıca SigDigger, SoapySDR sayesinde piyasadaki çoğu SDR cihazını desteklemektedir ve FSK, PSK ve ASK sinyallerinin ayarlanabilir demodülasyonuna, analog video kodunun çözülmesine, patlama sinyallerinin analiz edilmesine ve analog ses kanallarının (tümü gerçek zamanlı olarak) dinlenmesine olanak tanımaktadır.

SigDigger'ın, MacOS ve GNU/Linux desteği, hem gerçek zamanlı hem de tekrar analiz modları, analog mono ses çalma (AM, FM, LSB ve USB), temel bant kaydı (tam spektrum ve kanal başına), cihaz başına kazanç hediyeleri, dinamik spektrum tarama, ASK, FSK ve PSK denetimi, gradyan-iniş SNR hesaplaması, farklı spektrum kaynakları (siklostarioner analiz, sinyal gücü…), sembol kaydı ve görselleştirme, doppler analizi, dosya adı tabanlı ham dosya parametresi tahmini, geçiş analizi, etkileşimli panoramik spektrum görünümü, patlama algılama ve sınırlı çevrim dışı demodülasyon desteği dâhil olmak üzere dalga biçimi inceleme penceresi, sinyal kaynağı kırımı, bant planı bilgileri, ses kanalı kaydedici, kör parametre tahmini, demodüle edilmiş kanalın ağ yayını, alınan örneklerin ve demodüle edilmiş sembollerin UDP yayını, spektrum entegratörü (radyoastronomi meraklıları için) özellikleri mevcuttur.

SigDigger üç farklı projeye bağlıdır: Sigutils, Suscan ve SuWidgets. SigDigger'ı derlemeden önce bu uygulamaların derlenip kurulması gerekmektedir.

SigDigger'ı çalıştırmak için terminalde "*SigDigger*" komutu uygulanmaktadır. Hata ile karşılaşıldığında "*/opt/SigDigger/bin/SigDigger*" komutu uygulayarak SigDigger programı çalıştırılmaktadır. Program çalıştırıldaktan sonra alıcı ile vericinin belirlenen profile uygun kanaldaki frekans aralığına bağlı olarak iletişim kurduğu esnada SigDigger ile yakalanan ve Matlab, Octave v.d. yazılımların işlem yapabileceği ".m" formatında kaydedilen *panoramic tayf* sinyali Şekil 3.23'te verilmiştir.

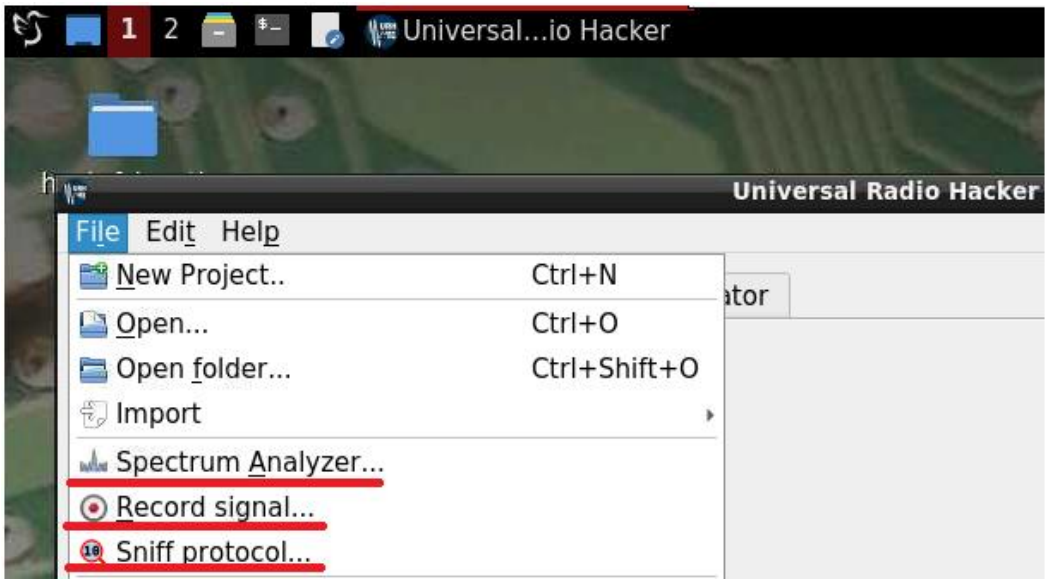


Şekil 3.23. SigDigger ile Wi-Fi panoramik tayf yakalama

3.2.5.3. Universal Radio Hacker (URH)

URH, RF parmak izi çalışmalarında kullanılmak üzere açık kaynak kodlu ve komut satırı tabanlı bir uygulamadır. Program, bir sinyalin frekans ve genlik özelliklerini analiz etmek, modülasyon türlerini tespit etmek, sinyalleri kaydetmek veya çıkarmak, sınıflandırmak veya karşılaştırmak gibi birçok işlemi gerçekleştirebilir. URH, protokol mantığına odaklanmak isteyen, HF ve Dijital Sinyal İşleme'nin derinliklerine dalmaktan kaçınmaya çalışan kuramsal odaklı araştırmacılar düşünülerek geliştirilmiştir (Pohl ve Noack, 2018).

Şekil 3.24'te URH ile yapılabilecek işlemler (*tayf analizi - spectrum analyser, sinyal kaydetme - record signal, sniff protocol v.d.)* verilmektedir. GNR uygulaması ile kayıt altına alınan veriler URH ile analiz edilebilmektedir.



Şekil 3.24. URH ile yapılabilecik işlevler

URH, RF *sinyallerini yakalama, sinyal analizi, sinyal yönlendirimi (manipülasyon) ve iletişim protokollerinin analizinde* kullanılmaktadır. URH, SDR donanımını kullanarak RF frekanslarında yayınlanan sinyalleri tespit edebilir ve bunları kaydedebilir. URH, yakalanan RF sinyallerini analiz etmek için bir dizi özellik ve araç sunar. Bu araçlar, sinyallerin frekansını, modülasyon türünü, veri formatını, bit hızını, paket yapısını ve diğer parametreleri belirlemek için kullanılabilir. URH, spektrum analizi, zaman alanı analizi, frekans alanı analizi ve paket analizi gibi çeşitli analiz yöntemleri sağlar. URH, yakalanan RF sinyallerini değiştirme ve tekrar gönderme yeteneği sağlar. Bu, RF sinyallerini çoğaltma, yeniden oynatma, yeniden yayınlama veya değiştirme gibi işlemleri içerir. Örneğin, bir kablosuz uzaktan kumandanın sinyalini yakalayabilir, ardından bu sinyali tekrar göndererek hedef cihazı kontrol edebilirsiniz. URH, iletişim protokollerini analiz etmek için kullanılabilir. RF tabanlı bir iletişim protokolünü inceleyebilir, protokol paketlerini ayıklayabilir, veri yapılarını analiz edebilir ve iletişim akışını anlayabilirsiniz. Bu, güvenlik açıklarını tespit etmek, protokolün çalışma mantığını anlamak veya mevcut protokolü ters mühendislik yapmak için kullanılabilir.

3.2.5.4. Inspectrum

Kayıt altına alınan sinyale ait tayf, açık kaynaklı işletim sistemlerinde Inspectrum aracı ile görüntülenerek analiz edilebilmektedir. Inspectrum, RTL-SDR veya HackRF gibi SDR'lerden oluşturulan IQ dosyalarıyla uyumludur. Şekil 3.24'te X ekseni FFT boyutu ile zamana bağlı olarak pencerenin örnek sayısını belirlemektedir. Bant genişliği, örnekleme frekansıyla değil, örnekleme hızıyla ilgilidir. Gerçek örneklemede, ~20MS/s'lik örnekleme

hızıyla, 10MHz'lik bir bant genişliği beklenmektedir ancak HackRF One karmaşık örnekleme yaptığından örnekleme oranı ile bant genişliği eşit olmaktadır. Şekil 3.25'de Y ekseni [-10MHz,+10MHz] örnekleme oranını ifade etmektedir.

Inspectrum'un desteklediği dosya türleri örnekleri:

*.sigmf-meta, *.sigmf-data - SigMF kayıtları

*.cf32, *.cfile - Karmaşık 32-bit kayan nokta örnekleri (GNU Radio, osmocom_fft)

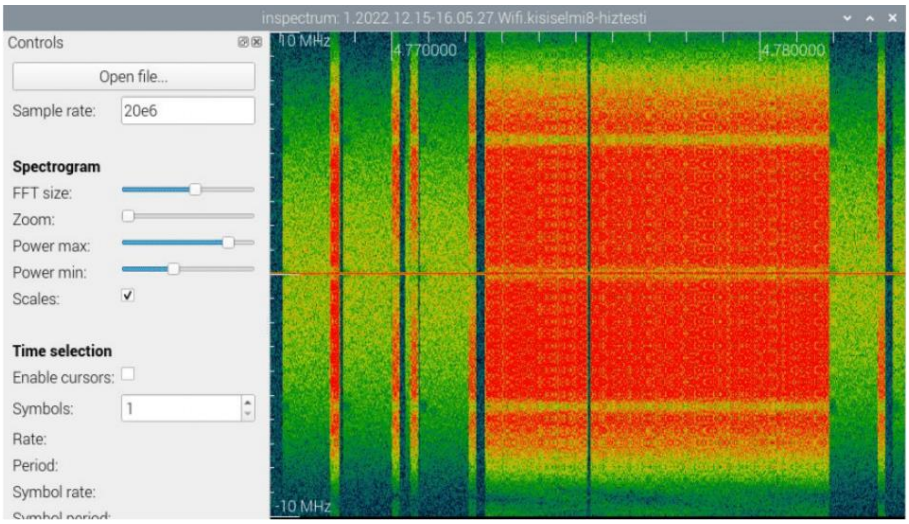
*.cs32 - Karmaşık 16 bit işaretli tamsayı örnekleri (SDRAngel)

*.cs16 - Karmaşık 16 bit işaretli tamsayı örnekleri (BladeRF)

*.cs8 - Karmaşık 8 bit işaretli tamsayı örnekleri (HackRF)

*.cu8 - Karmaşık 8 bitlik işaretsiz tamsayı örnekleri (RTL-SDR)

*.f64 - Gerçek 64-bit kayan nokta örnekleri (Matlab)



Şekil 3.25. inspectrum aracı ile tayf analizi

3.2.6. Açık kaynak ağ analiz ve diğer kullanılan yardımcı araçlar

Ağ analiz araçları, ağdaki trafiği dinlemek, analiz etmek ve anlamlandırmak için kullanılmaktadır. Wireshark, tcpdump, Suricata, Snort, Zeek, nmap, OSSEC v.d. yaygın olarak kullanılan açık kaynak kodlu ağ analiz yazılım araçlarıdır.

Wireshark, bir ağın içindeki trafiği dinleyebilir, kaydedebilir ve analiz edebilir. Wireshark, ağ güvenliği sorunlarını tespit etmek, ağ performansını değerlendirmek, ağın genel

işleyişini anlamak ve ağ sorunlarını gidermek için de kullanılır. Ağ paketlerini çözümler, protokolleri ait detaylı istatistikler sunar ve ağ trafiğinin görselleştirilmesine imkan sağlar.

Tcpdump, Unix tabanlı sistemlerde yaygın olarak kullanılan komut satırı ağ analiz aracıdır. Ağ paketlerinin yakalanması, dinlenmesi ve kaydedilmesinde kullanılır. Wireshark'a göre daha sade bir araçtır, komut satırında hızlı ve etkili çözümler sağlar.

Suricata ve Snort, ağ tabanlı saldırıları tespit etmek ve ağ trafiğini izlemek için kullanılır. Açık kaynaklı saldırı tespit (IDS) ve önleme (IPS) aracıdır.

Zeek, ağ trafiğini izler ve ağ olaylarına ilişkin bilgileri ayrıntılı olarak günlüğe kaydeder.

Nmap (network mapper), ağda bulunan cihazlar için port ve ağ taraması yapar. Hızlı bir şekilde ağı haritalar ve ağda çalışan servislerin durumunu kontrol eder.

4. RF PARMAK İZİ TANIMA İÇİN ÖZNİTELİK BELİRLEME

Sinyal gürültü oranının (SNR) yüksek olması RF parmak izi oluşturmak için daha avantajlıdır çünkü, yüksek SNR, sinyalin gürültüden daha iyi ayrılmasını sağlamaktadır. Bu, sınıflandırmada daha hassas öznitelikler elde edilmesini mümkün kılar. Sınıflandırmada, *frekans spektrumu, zaman/frekans aralığı ve modülasyon türü* öznitelikleri kullanılmaktadır.

Sinyal için *frekans spektrumu*, sinyalin genliği veya band genişliği gibi özellikleri belirlemektedir. Sinyal için *zaman/frekans aralığı*, sinyalin zaman içinde değişen frekans spektrumu gibi özellikleri belirler. Sinyal için *modülasyon türü,* sinyalin nasıl modüle edildiğini ifade etmektedir. Ayrıca bu öznitelikleri elde edebilmek için *Fourier dönüşümü, Wigner-Ville dönüşümü, demodülasyon algoritmaları* kullanılmaktadır. Sinyalin frekans spektrumunu elde etmek için *Fourier dönüşümü* kullanılmaktadır. Sinyalin zaman/frekans aralığını elde etmek için *Wigner-Ville dönüşümü* kullanılmaktadır. Sinyalin modülasyon türünü elde etmek için *demodülasyon algoritmaları* kullanılmaktadır,

RF sinyalinden öznitelik çıkarmada kullanılan yöntemler arasında Fourier dönüşümü, Wavelet dönüşümü, PCA (Principal Component Analysis) ve ICA (Independent Component Analysis) gibi algoritmalar yer almaktadır. Bu algoritmalar sinyalin spektrumunu veya sinyalin zamansal bileşenlerini inceleyerek, sinyal içinde bulunan özellikleri çıkarır. Bu özellikler sınıflandırmada kullanılabilir. Ayrıca, Hilbert dönüşümü RF sinyalinden özellik çıkarmada kullanılabilir. Örneğin, Hilbert dönüşümü kullanarak RF sinyalinde zaman-frekans analizi yapmak mümkündür. Bu analiz yöntemi, sinyalin frekans bileşenlerinin zaman içinde nasıl değiştiğini ve frekans bileşenlerinin ne kadar güçlü olduğunu gösterir. Bu bilgi, sinyal sınıflandırması ve tanıma işlemlerinde kullanılabilir.

4.1. Öznitelik Belirleme Yaklaşımları

RF sinyal özniteliklerini belirlemek için sinyalin preamble (öncül), transient (geçici) ve steady-state (kararlı hal) durumlarından faydalanılır. Bu bölümde öznitelikler belirlenirken kullanılacak yaklaşımlar detaylı açıklanmıştır.

4.1.1. Geçici (transient) temelli

Bayesian Step Change Detection (BSCD), sinyalin ardışık bölümleri için fraktal boyutun varyansını hesaplamak için Higuchi'nin yöntemini kullanan bir yaklaşıma dayanmaktadır

(Higuchi, 1988). Şekil 4.1'de BSCD verilmektedir. Burada, iki ardışık dizi arasındaki fraktal boyutun varyansı, onların posteriori olasılık dağılım fonksiyonu (ppDF) ile orantılıdır. Olasılık dağılım fonksiyonundan (pDF) elde edilen maksimum değer daha sonra geçişin başlangıcı olarak belirlenir (Higuchi, 1988). Bu yöntemin ilk adımında, örneklerin alt kümeleri Eşitlik (4.1)'deki gibi yeniden düzenlenir:

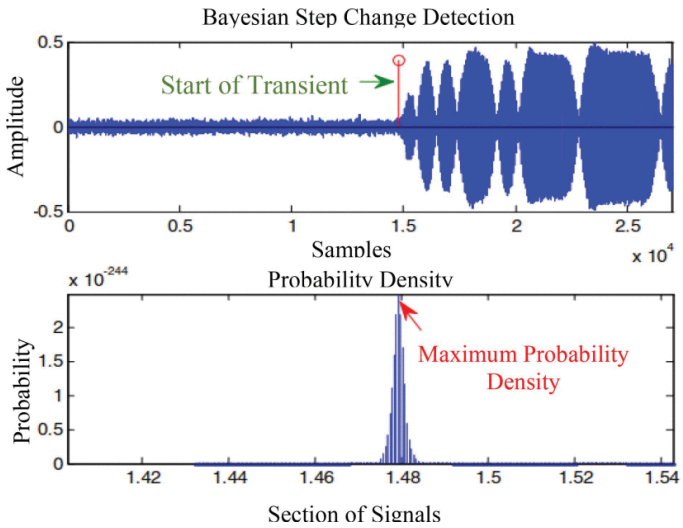
$$X(m,k): X(m), X(m+k), \ldots, X\left(m + \left[\frac{N-m}{k}\right] \times k\right) \tag{4.1}$$

Eşitlik (4.1)'de $X(m,k)$ altküme aralığıdır, m başlangıç zamanıdır ve k aralık zamanıdır.

Her bir alt küme için eğrinin uzunluğu, $L_m(k)$, daha sonra Eşitlik (4.2) ile hesaplanır:

$$L_m(k) = \left\{\left(\sum_{i=1}^{\frac{N-m}{k}} | X(m+ik) - X(m-(i-1)k |\right) \times \frac{N-1}{\left[\frac{N-m}{k}\right]k}\right\}/k \tag{4.2}$$

Daha sonra, k setinin $L_m(k)$ ortalama değeri bir log-log ölçeğinde çizilir. Daha sonra eğri uydurma gerçekleştirilir ve eğrinin eğimi fraktal boyut olarak değerlendirilir.



Şekil 4.1. BSCD

Kaynak: (Huang vd., 2013)

Son adımda, ppDF takip edilerek Eşitlik (4.3)'ten geçişin (m) başlangıcı tespit edilir.

$$P(\{m\} \mid d) \propto \frac{1}{\sqrt{m(N-m)}}\left[\sum_{i=1}^{N} d_i^2 - \frac{1}{m}\left(\sum_{i=1}^{m} d_i\right)^2 - \left(\frac{1}{N-m}\right)\left(\sum_{i=m+1}^{N} d_i\right)^2\right]^{\frac{N-2}{2}} \quad (4.3)$$

Eşitlik (4.3)'te N, kayan penceredeki örnek sayısıdır, d ise fraktal boyutu belirtmektedir.

Bayesian Ramp Change Detection (BRCD), Ureten ve Serinken tarafından önerilmiştir (O Üreten ve Serinken, 2005) ve BSCD şemasının bir modifikasyonudur. Bu yaklaşımda, sinyal gücünün yavaşça arttığı zaman anını tahmin ederek geçici durum tespiti elde edilir. Daha önce bahsedildiği gibi, tipik iletim verileri, gerçek verilerin iletiminden önce kanal gürültüsünü içerir. Bu sinyalin modeli Eşitlik (4.4)'te verilen bir matris denklemi şeklinde yazılabilir:

$$d = Gb + e \quad (4.4)$$

d, veri örneklerinin bir N×1 matrisidir; e, N×1 boyutlarına sahip Gauss gürültü örneklerinin bir matrisidir, G matrisi N×M boyutundadır ve G'nin her sütunu, aşağıdaki her örnekte tahmin edilen bir temel fonksiyondur. Zaman serisi ve b, doğrusal katsayıların bir M×1 matrisidir. Bir sonraki adım, Eşitlik (4.5)'te (O Üreten ve Serinken, 2005) olduğu gibi hesaplanan bir posteriori olasılık yoğunluğu ile değişim noktasının tespit edilmesidir:

$$p(\{m\} \mid d, I) \propto \frac{\left[d^T d - d^T G\left(G^T G\right)^{-1} G^T d\right]^{-(N-m)/2}}{\sqrt{\det(G^T G)}} \quad (4.5)$$

Eşitlik (4.5)'de I, sinyal modelini tanımlar. Başlangıç noktası konumu, Eşitlik (4.6)'da verilen G matrisinin yapısında bulunabilir.

$$G^T = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 2 & 3 & \cdots & N-m \end{bmatrix} \quad (4.6)$$

Bayesian ramp change detector (BRCD) (Ureten ve Serinken, 2007), geçici sinyalin başlangıç noktasının gerisindeki gecikmeler ve algılamanın standart sapması nedeniyle Bayesian adım değişim detektörüne kıyasla Wi-Fi radyoları için geçici çıkarım için daha iyi bir adaydır. BSCD için hata, BRCD'den üç kat daha yüksektir.

Variance Fractal Dimension Threshold Detection (VFDTD), 1997 yılında Kanada'da Manitoba Üniversitesi'nde Profesör D.Shaw ve Profesör W. Kinsner tarafından ortaya

atılmıştır; sinyal genliğinin varyansından fraktal boyutu hesaplayarak Wi-Fi verici geçici olaylarını algılar. Ayrıca, VFDTD'nin uygulanması Eşitlik (4.7) gibidir:

İlk olarak, kayan pencere ile bölütlenen her bir sinyalin fraktal boyutu $D(t)$ hesaplanmaktadır.

$$D(t) = 2 - H \tag{4.7}$$

burada H Hurst indeksidir, ΔX(ti, Δt) ve Δt arasındaki korelasyonu temsil eder; ΔX(ti, Δt) sinyalin herhangi bir noktası arasındaki genlik farkını temsil eder, yani ΔX(ti,Δt)=X(ti+Δt)−X(ti) ve Δt=|ti+1 – ti| . Hurst indeksi, en küçük kareler regresyon yöntemine dayanan Eşitlik (4.8) ile hesaplanır.

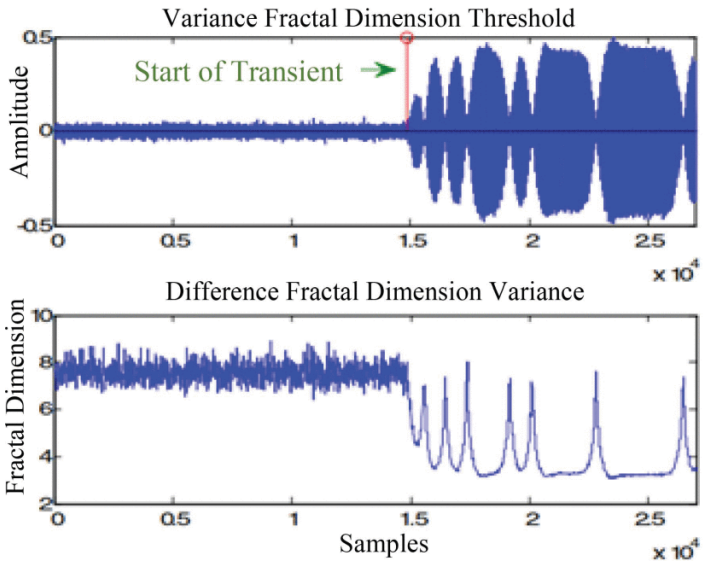
$$2H = \frac{N\sum_{i=1}^{N} x_i y_i - \left(\sum_{i=1}^{N} x_i\right)\left(\sum_{i=1}^{N} y_i\right)}{N\left(\sum_{i=1}^{N} x_i^2\right) - \left(\sum_{i=1}^{N} x_i\right)^2} \tag{4.8}$$

Eşitlik (4.8)'de, (x_i, y_i) = (log (Δti), log (var (ΔX (ti, Δti))))). Uygun bir zaman dizisi seçmek çok önemlidir ve yeterli (x_i, y_i)) çifti olduğundan emin olmak gerekir.

Bir sonraki adım, ilk adımdan elde edilen fraktal boyuttan geçici sinyalin başlangıç noktasını tespit etmektir ve daha sonra eşik τ, kanal gürültüsünün fraktal boyutunun ortalaması olarak ayarlanır. Geçerli noktanın değeri ve ardışık 450 noktadan sonraki τ eşiğinden küçükse, o zaman n, geçişin başlangıcı olarak değerlendirilmektedir.

$$D(n), D(n+1), \ldots, D(n+450) \leq \tau \tag{4.9}$$

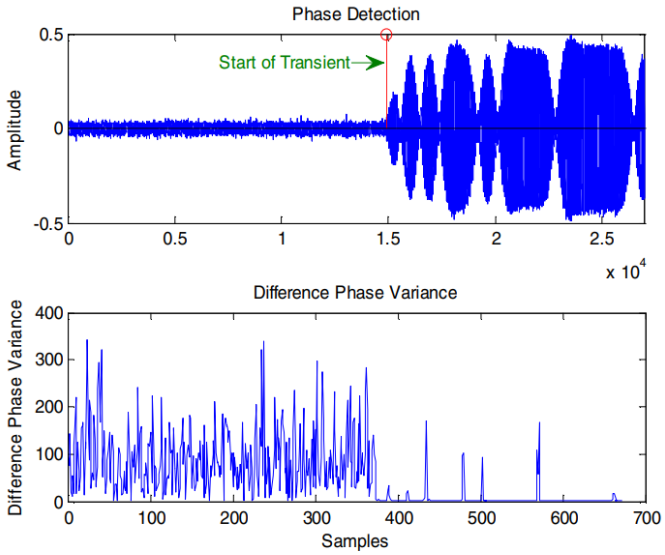
Kablosuz ağ kartı net çekirdeğinin geçici ve fraktal yörüngesinin başlangıcı Şekil 4.2'de gösterilmektedir, kanal gürültüsünün fraktal boyutu ile geçici sinyal arasında önemli bir fark olduğu görülebilir bu nedenle başlangıç noktasının konumu buradan tespit edilebilir. Bu yöntem basit ve hızlıdır ancak eşiğin deneme yanılma yoluyla belirlenmesi gerekir ve gürültüye karşı çok hassastır.



Şekil 4.2. net-core sinyal örneğinin BSCD'si

Kaynak: (L. Huang vd., 2013)

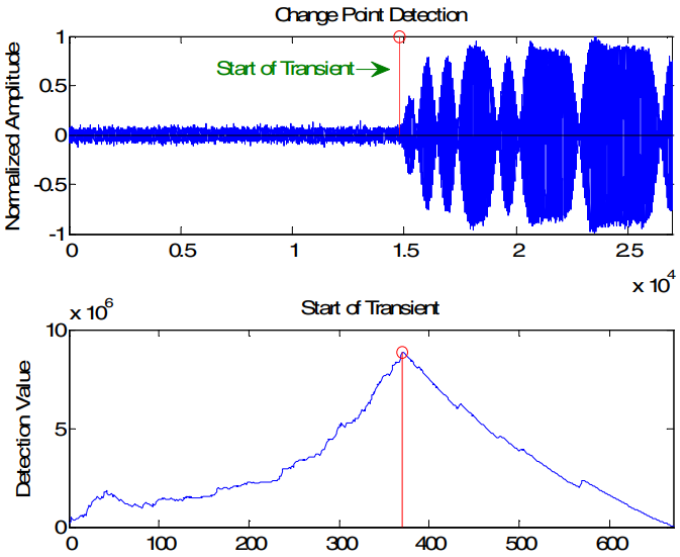
Phase Detection (PD), 2003 yılında I. Hall vb. tarafından önerilmiştir (Hall vd., 2003), tespit amacıyla faz özelliklerinden yararlanır. Prensibi şu şekildedir: Analitik sinyal, gerçek sinyalin Hilbert dönüşümü ile alınabilir.



Şekil 4.3. net-core sinyal örneğinin PD'si

Kaynak: (L. Huang vd., 2013)

Mean Change Point Detection (MCPD), yönteminde örneklerin istatistiği arasındaki fark büyütülür ve maksimum farkı veren konum geçiş başlangıcı olarak belirlenir (Huang vd., 2013).



Şekil 4.4. net-core sinyal örneğinin MCPD'si

Kaynak: (L. Huang vd., 2013)

Permutation Entropy (PE) and Generalized Likelihood Ratio Test (GLRT) Detector, permütasyon entropisi (PE) ve genelleştirilmiş olabilirlik oranı testi (GLRT) dedektörüne dayalı bir zamansal sinyali tespit eder (Yuan vd., 2015). Permütasyon Entropisi (PE), Bandt-Pompe tarafından tanıtıldı ve zaman serilerinin düzensizliğini ve karmaşıklığını değerlendirebilir (Cao vd., 2004). PE basit, yapısal olarak sağlam ve hızlıdır.

Superiority of Energy Criterion (EC), akustik ve elektromanyetik kısmi deşarjları tespit etmek için iyi bilinen bir tekniktir. Çeşitli uygulamalarda sinyallerin varış zamanını tahmin etmek için yaygın olarak kullanılır. EC'nin altında yatan fikir, bir sinyalin gelişinin, enerji içeriğinin bir varyasyonu ile karakterize edilmesidir. Örneklenmiş bir sinyalin (x) enerjisi (Ei), genlik değerlerinin kümülatif toplamı olarak tanımlanır (Markalous vd., 2008), (Herold vd., 2007).

4.1.2. Geçici (transient) olmayan temelli

Kararlı durum tabanlı yaklaşımlar, sinyalin modüle edilmiş kısmından çıkarılan benzersiz özelliklere odaklanır. Gerdes v.d. aynı model ve üreticinin kartlarını tanımlayabilen kararlı durum tabanlı bir RFF tekniği önerdi. IEEE Ethernet 802.3'ün giriş kısmı (3 farklı modele sahip 16 cihaz), sinyalin yayıldığı cihazı tanımlamaya yardımcı olan cihaz parmak izi profilini sağlamak için kullanıldı. Sınıflandırmayı sağlamak için eşleşen bir filtre uygulaması ve basit bir eşik kullanılmıştır. Bu cihazlar için analog sinyallerin özelliklerinin izlenebilir

olduğunu ve ayrıca ağ erişim kontrol şemaları için uygun olduğunu göstermişlerdir (Gerdes vd., 2006). Brike et al. modüle edilmiş sinyalin beş özel özelliğini kullanan bir Pasif Radyometrik Cihaz Tanımlama Sistemi (PARADIS) önerdi. Frekans hatası, SYNC (senkron) korelasyon, I/Q orijin ofseti ve fiziksel katman tanımlaması için büyüklük ve faz hataları özelliklerini SVM ve k-NN sınıflandırıcı ile sınıflandırılan bir RF parmak izi profili yapmak için kullanıldı. Sistem, sınıflandırıcıların doğruluğunu test etmek için antenden 3 ila 15 m mesafede bir üst düzey vektör sinyal analizörü tarafından yakalanan 138 özdeş model IEEE 802.11b sinyalini kullandı (Brik vd., 2008). Shi ve Jensen, PARADIS'e benzer bir yaklaşım önerdi ve çoklu giriş çoklu çıkış cihazlarını tanımlamak için modülasyon alanındaki radyometrik özellikleri kullandı. RFID cihazlarını sınıflandırmak için modülasyon tabanlı yöntemler de kullanılmıştır (Shi ve Jensen, 2011). Danev et al. ayrıca modülasyon şeklinden çıkarılan öznitelikleri ve RFID aktarıcılarından spektral öznitelikleri kullandı. Önerilen yöntem (ISO 14443, HF 13.56 MHz), RFID aktarıcısının 4 farklı sınıfı ve farklı modeli üzerinde test edilmiştir (Danev vd., 2009). Birçok çalışmada, vericileri tanımlamak için frekans alanı özellikleri kullanılmıştır. Laboratuvar deneyleri için sekiz Evrensel Radyo Çevre Birimi (USRP) vericisi kullanıldı. Bu makale, geleneksel bir ayırt edici sınıflandırıcı (k-NN) ile esnek özellik seçimi kullanarak mükemmel bir performans iyileştirmesi sunar. Yaklaşım, 30dB SNR'de %97 doğrulukla iyi performans gösterir ve performans, 0dB SNR'de %66 doğrulukla hala iyidir (Kennedy vd., 2008). Suski ve ark. Güç Spektral Yoğunluk (PSD) katsayılarını, IEEE 802.11a/g sinyalinin giriş kısmından benzersiz özellikler olarak kullandı (Suski II vd., 2008a). Başlangıçta, araştırma daha çok geçici-tabanlı RF parmak izi ile ilgiliydi çünkü sinyalin sabit durum kısmı tüm vericiler için ortak değildir. Geçici sinyal her zaman bir iletimde meydana gelir, bu nedenle araştırma geçici durum tabanlı yaklaşımlara odaklanmıştır. Bununla birlikte, kısa periyodu ve fazın güvenilirliği nedeniyle geçici sinyali çıkarmak için daha yüksek bir örnekleme hızı gereklidir ve genlik bilgisi bu alanda ciddi bir zorluktur (Kennedy vd., 2008). Halihazırda bu yaklaşımlar için kararlı durum sinyallemesine ihtiyaç duyulmamaktadır, çünkü neredeyse tüm kablosuz yerel alan ağları (WLAN), RFID vb. alıcı tasarımını basitleştirmek için veri iletiminin başlangıcında bir girişi vardır (Scanlon vd., 2010).

4.1.3. Diğer yaklaşımlar

Önerilen fiziksel katman tanımlama tekniklerinden bazıları bahsedilen sınıflandırma ile ilişkilendirilememiştir (Jana ve Kasera, 2009), (Klein vd., 2009). Bu yaklaşımlar genellikle tescilli bir kablosuz teknoloji kullanır ve/veya sinyalin ve mantıksal katmanın diğer özelliklerini

çıkarır. Danev v.d. fiziksel katman tanımlaması için, zamanlama ve modülasyonun yalnızca farklı üreticilere ait cihazları ayırt ettiğini, ancak spektral özelliklerin aynı üretici ve modele ait cihazları tanımlamak için tercih edilen bir parmak izi olacağını gösterdi (Danev vd., 2009). Jana ve Kasera, kablosuz yerel alan ağındaki erişim noktalarını (AP'ler) tanımlamak için benzersiz bir özellik olarak saat eğriliğini kullandı (Jana ve Kasera, 2009). Bu tekniğin etkinliği karmaşık ağlar için gösterilmiştir (Kohno vd., 2005). Sonuçlar, farklı AP'lerin yüksek doğrulukla ayırt edilebileceğini gösterdi. (Klein vd., 2009), (Klein vd., 2010), IEEE 802.11a (OFDM) cihazlarını tanımlamak için karmaşık bir dalgacık dönüşümü uygulandı. Çıkarılan öznitelikleri sınıflandırmak için kullanılan Çoklu Ayrım Analizi (MDA) ve bu yaklaşım için sınıflandırma başarımı aynı model 4 Cisco kablosuz cihaz üzerinde test edilmiştir. Sonuçlar, 8 dB SNR iyileştirmesi için %20 sınıflandırma hata oranı gösterdi. Suski ve ark. (Suski II vd., 2008b) kablosuz cihazları benzersiz bir şekilde tanımlamak için IEEE 802.11a'nın giriş kısmının güç spektrum yoğunluğunu (PSD) ölçerek bir RF parmak izi profili oluşturur. Bu yaklaşım 3 cihaz üzerinde test edildi ve SNR'si 6 dB'den büyük olan yakalanan paket çerçeveleri için %20'lik bir ortalama sınıflandırma hatası oranına ulaştı. Son araştırmalar, fiziksel katman tanımlaması için farklı RFID sınıflarını hedef almıştır (Zanetti vd., 2010), (Periaswamy vd., 2010). Periaswamy ve ark. (Periaswamy vd., 2010), (Chinnappa Gounder Periaswamy vd., 2010), cihaz tanımlaması için UHF RFID etiketlerini kullandı. Yazarlar, minimum güç yanıtı özelliğinin cihazları %94,4 (%0,1 Yanlış Kabul Oranı (FAR ile) ve %90,7 (FAR ve FAR ile %0,2) arasında iki farklı 50 etiketlik iki bağımsız kümeyi tanımlamak için kullanılabileceğini gösterdi. Son zamanlarda araştırmacılar GSM cihazlarında çeşitli sinyal karakteristiklerini, sinyal parçalarını (Reising vd., 2010), (Williams vd., 2010), (Williams vd., 2010) araştırmışlardır. 4 farklı üreticinin cihazlarını tanımlamak ve sınıflandırmak için GSM-GMSK patlama sinyallerinin ara ve geçici kısmını kullandılar. Sonuçlar, orta seviye kısım kullanıldığında sınıflandırma doğruluğunun keskin bir şekilde düştüğünü, ancak, yakın zamansal kısmın GSM sinyallerini tanımlamak için uygun olduğunu gösterdi.

4.2. Anlık Faz, Frekans ve Genlik

Bir sinyalin AG, AFa ve AFr değerleri, Hilbert dönüşüm olarak bilinen bir işlemle belirlenir. Eşitlik (4.10), $-\infty < t < +\infty$ aralığında tanımlanmış bir gerçek değerli $\hat{x}(t)$ ile orijinal $x(t)$ sinyali için HD'yi ifade eder.

$$\hat{x}(t) = \mathrm{H}\{x(t)\} = \int_{-\infty}^{\infty} \frac{x(\tau)}{\pi(t-\tau)} dt \tag{4.10}$$

Bir sinyalin HD'si, orijinal sinyalden 90° faz kayması olan ortogonal bir sinyal verir (Ktonas ve Papp, 1980; Manjula vd., 2013). Picibono, x(t) sinyalinin analitik biçimini tanımlar ve bu ifade Eşitlik (4.11)'de verilmektedir (Picinbono, 1997).

$$z_x(t) = x(t) + j\hat{x}(t) \tag{4.11}$$

Analitik form kullanılarak, IA $a_x(t)$, IP $\Phi_x(t)$ ve IF $f_x(t)$ değerleri (4.12)-(4.14) eşitlikleriyle ifade edilmektedir.

$$a_x(t) = |z_x(t)| = \sqrt{x(t)^2 + \hat{x}(t)^2} \tag{4.12}$$

$$\Phi_x(t) = \arctan\left(\frac{\hat{x}(t)}{x(t)}\right) \tag{4.13}$$

$$f_x(t) = \frac{1}{2\pi}\left[\frac{d\Phi_x(t)}{dt} mod(2\pi)\right] \tag{4.14}$$

AFa değeri, bir sinyalin zaman içindeki dalga formunun o anki zaman anında bir referans sinyaline göre ne kadar geride veya önde olduğunun ölçüsüdür. Faz, periyodik bir sinyalde aynı zamanda frekansın bir ölçüsüdür ve sinyalin bir periyodunun tamamlanması için geçen süreyi ifade eder. AFa değeri, bir sinyalin dalga formunun anlık durumunu ifade eder. Bu değer, bir referans sinyali ile karşılaştırılarak hesaplanır. Örneğin, bir sinüs sinyalinin AFa değeri, referans sinüs sinyaline göre, o anki zaman anında ne kadar geride veya önde olduğunu ifade eder. AFa değeri, birçok alanda kullanılır. Örneğin, elektromanyetik dalgalarda, ses dalgalarında, veri iletiminde ve kontrol sistemlerinde kullanılır. Birçok elektronik cihazda sinyallerin doğru zamanlama ve senkronizasyonu için AFa değeri çok önemlidir. AFa değeri, genellikle radyo frekans ve diğer elektriksel sinyallerin ölçümlerinde kullanılır. RF sinyallerinin faz durumu, sinyallerin birbirleriyle etkileşimini ve bilgi taşıma kapasitesini etkileyebilir. AFa değerinin doğru bir şekilde ölçülmesi, RF mühendisleri ve diğer teknisyenlerin sinyalleri doğru bir şekilde analiz etmelerine ve iletim hatası oluşumunu önlemelerine yardımcı olabilir.

AFr değeri, bir sinyalin dalga formunun zaman içindeki değişim hızının ölçüsüdür. Frekans, bir sinyalin tekrarlanan periyodik hareketlerinin sayısıdır ve genellikle Hz (Hertz) olarak ifade edilir. AFr değeri, bir sinyalin dalga formunun anlık durumunu ifade eder. Bu değer, sinyalin AFa değerindeki değişimlere göre hesaplanır. AFr, bir sinyalin dalga formunun

herhangi bir anında frekans değişim oranını ifade eder. AFr, sinyalin spektral bileşenleri ve spektrum analizleri gibi birçok uygulamada kullanılır.

AFr hesaplamak için, bir sinyalin zamanla değişen faz değerlerini elde etmek gerekir. Bu faz değerlerinin zaman türevi alınarak, AFr değerleri elde edilebilir. Yani, AFr değeri, bir sinyalin fazı ile zamanın türevi arasındaki orandır. AFr değeri, birçok alanda kullanılır. Örneğin, radyo ve TV sinyallerinde, ses işlemede, tıp alanında, manyetik rezonans görüntülemede (MRI) ve radar gibi uygulamalarda kullanılır. AFr değeri, sinyallerin analizi, işlenmesi ve sentezi için çok önemlidir.

Bir sinyalin AFr, sinyalin dalga formu hakkında önemli bilgiler sağlar. Örneğin, sinyalin dalga formu karmaşık bir yapıya sahipse, AFr sinyalin bu yapıdaki değişimlerini anlamak için kullanılabilir. AFr ayrıca, bir sinyalin doğru bir şekilde işlenmesi ve iletilmesi için önemlidir.

AG değeri, bir sinyalin anlık durumundaki maksimum genlik değerini ifade eder. Genlik, bir sinyalin dalga formunun en yüksek noktası ile en düşük noktası arasındaki mesafedir. AG değeri, bir sinyalin dalga formunun herhangi bir anında genlik değişim oranını ifade eder.

AG değeri, birçok uygulamada kullanılır. Örneğin, ses işlemede, manyetik rezonans görüntülemede (MRI) ve radar gibi uygulamalarda kullanılır. AG değeri, bir sinyalin işlenmesi ve iletilmesi için çok önemlidir.

Bir sinyalin AG değeri, sinyalin anlık durumunu ifade eder. Örneğin, bir sinüs sinyalinin AG değeri, sinyalin dalga formunun en yüksek veya en düşük noktasına göre ne kadar büyük veya küçük olduğunu ifade eder. AG değeri, sinyallerin analizi ve işlenmesi için önemlidir. Bir sinyalin AG değeri, sinyalin gücü ve işaretin zayıflaması gibi konular hakkında önemli bilgiler sağlayabilir.

AG değeri, bir sinyalin RMS (Root Mean Square) değerinin hesaplanmasında da kullanılır. RMS değeri, bir sinyalin genliğinin ortalama karekök değeridir ve bir sinyalin gerçek genliğini daha doğru bir şekilde ölçer. AG değeri, RMS hesaplamalarında sinyalin dalga formunun anlık durumunu ifade ettiği için önemlidir.

AG değeri, bir sinyalin doğru bir şekilde işlenmesi ve iletilmesi için önemlidir. Sinyallerin işlenmesi sırasında, AG değerleri dikkate alınarak filtreleme, amplifikasyon ve

diğer işlemler yapılır. Ayrıca, sinyallerin iletilmesi sırasında, AG değerleri, sinyalin iletilmesi için gerekli gücü belirlemeye yardımcı olur.

4.3. İstatistiksel Öznitelikler

Sınıflandırmada basıklık, çarpıklık, varyans, standart sapma, aritmetik ortalama, geometrik ortalama v.b. istatistiksel yöntemler/öznitelikler kullanılmaktadır. Bu yöntemler ve ilgili özniteliklerin hesaplanmasında kullanılan eşitlikler Tablo 4.1'de verilmektedir.

Basıklık (kurtosis), bir veri dağılımının yayılımının, simetrisinin ve kuyruklarının ölçüsüdür. Radyo frekans basıklığı, RF sinyallerinin istatistiksel analizi, sinyal tespiti, radyo haberleşmesi, radyo frekans spektrum algılama ve diğer RF uygulamalarında kullanılan bir ölçüttür. Yüksek radyo frekans kurtosis değerleri, sinyallerin Gaussian olmayan özelliklerini yansıtabilir. Örneğin, RF sinyallerinde yüksek basıklık değerleri, sinyallerin aniden yüksek veya düşük değerlere sahip olabileceğini, ani dalgalanmalar veya sinyal yoğunluğundaki değişimleri işaret etmektedir.

Tablo 4.1. Sınıflandırma süreçlerinde kullanılan istatistiksel öznitelikler ve eşitlikleri

Numara	Yöntem/Öznitelik	Eşitliği
1	Aritmetik ortalama (Aort)	$\frac{1}{N}\sum_{n=1}^{N}\lvert F(n)\rvert$
2	Geometrik ortalama (Gort)	$\sqrt{\prod_{n=1}^{N}\lvert F(n)\rvert}$
3	Harmonik ortalama (Hort)	$\frac{N}{\sum_{n=1}^{N}\frac{1}{\lvert F(n)\rvert}}$
4	Standart sapma (Std)	$\sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})}$
5	Çarpıklık (skewness)	$\frac{1}{N}\sum_{n=1}^{N}\left(\frac{\lvert F(n)\rvert - Aort}{Std}\right)^3$
6	Basıklık (kurtosis)	$\frac{1}{N}\sum_{n=1}^{N}\left(\frac{\lvert F(n)\rvert - Aort}{Std}\right)^4$

7	Varyans (variance)	$\frac{1}{N}\sum_{n=1}^{N}\left(\frac{\lvert F(n)\rvert - Aort}{Std}\right)^2$

Çarpıklık (skewness), bir veri dağılımının simetrisini ölçen bir istatistiksel terimdir. Radyo frekans çarpıklık değeri, RF sinyallerinin simetrisini ve dağılım özelliklerini değerlendirmek için kullanılmaktadır. Yüksek çarpıklık değerleri, sinyallerin sağa veya sola çekik olduğunu ve dağılımın simetrik olmadığını gösterebilir. Bu bilgi, sinyal analizi, modülasyon tanıma, sinyal tespiti ve diğer RF uygulamalarında kullanılabilmektedir.

Varyans (variance), bir veri kümesindeki verilerin ne kadar yayıldığını ölçen bir istatistiksel terimdir. RF sinyallerinin varyansı, sinyalin gücü veya şiddeti hakkında bilgi sağlar. Yüksek varyans değerleri, sinyalin geniş bir güç aralığına sahip olduğunu gösterirken, düşük varyans değerleri daha sınırlı bir güç aralığını işaret etmektedir.

Standart sapma, bir veri kümesindeki verilerin ortalamadan ne kadar uzaklaştığının ölçüsüdür. RF sinyallerinin standart sapması, sinyalin dalgalanma, değişkenlik veya çeşitlilik düzeyi hakkında bilgi sağlar. Yüksek standart sapma değerleri, RF sinyalinin geniş bir güç veya şiddet aralığına sahip olduğunu gösterirken, düşük standart sapma değerleri daha homojen bir güç dağılımını işaret etmektedir.

4.4. Veri Kümesi ve Özellik Çıkarımı

Bu bölümde, veri kümesini oluşturan IoT cihazlar hakkında bilgilendirmeler verilerek bu çalışmada kullanılan özellik çıkarım yöntemleri tanımlanmış ve gerekli bilgiler özetlenmiştir. Tablo 4.2, veri kümesi oluşturulmasında kullanılan IoT cihazları hakkında bilgi içermektedir. Özellik çıkarma işleminde ham sinyalin geçici bölgesi/kısmı (fazın aniden değiştiği kısım) tespit edildikten sonra HD ile AG, AFa ve AFr değerlerine kısıtlamalar uygulanarak öznitelikler belirlenir. MRMR ile özellik azaltma işlemi, bu özelliklerden etkin bir grup seçilerek gerçekleştirilir.

Tablo 4.2. Veri kümemizde RF sinyalleri yakalanan IoT cihazları hakkında bilgiler

Sınıf	Cihaz	Tür	Wi-Fi Çip Üzerinde Sistem (SoC)	Wi-Fi MAC	Wi-Fi Desteği
11	Xioami RedmiNote8	Akıllı telefon	MT7620A	1CCCD606D9**	Wi-Fi 5
22	RPi-4	Tek kart bilgisayar	BCM43438/CYW43438	E45F01478C**	Wi-Fi 5
33	RPi-3B+	Tek kart bilgisayar	BCM43143	B827EBF1A7**	Wi-Fi 5

44	RPi-400	Tek kart bilgisayar	BCM43456	E45F01061D**	Wi-Fi 5
55	Lenovo Tab M10	Tablet	MT6762 Helio P22T	FE4AA888E0**	Wi-Fi 5
66	RPi-3B+	Tek kart bilgisayar	BCM43143	B827EB592C**	Wi-Fi 5
77	DN-7042-1	Usb Wi-Fi genişletici	RTL8188CU	00E04C0BB0**	Wi-Fi 4

Tablo 4.3, IoT cihazları ve erişim noktaları arasındaki Wi-Fi iletişimi yoluyla elde edilen orijinal veri kümemizin özelliklerini göstermektedir. Cihazların her biri, kaydedilen toplam 3752 sinyal için yaklaşık 520–550 kayıt vermektedir. Veri kümesini oluşturmak için aşağıdaki adımlar izlenmektedir:

- Her cihaz için ortalama 520-550 kayıt bulunmaktadır. Her kayıt, 1 milyon ham karmaşık sinyal veri kaydı içerir.
- Zirve değeri, karmaşık sinyalin mutlak değeri alınarak hesaplanır. Geçici bölge/bölüm, tepe değerinden önceki 200 örnekle temsil edilir.
- 2000 örnek sayısı elde etmek için geçici sinyalin örnekleme oranı on kat artırılır.
- Pencere gezinme mantığı kullanılarak her kayıttaki 2000 örneği 125'erli gruplar halinde 16 farklı alt gruba ayırılır.
- HD'yi her gruptaki 125 örnek üzerinde çalıştırarak sırasıyle AG, AFa ve AFr değerleri elde edilir (AG, AFa ve AFr başına 16 örnek).
- Tablo 4.3'de AG, AFa ve AFr değerlerine Tablo 4.1'deki istatistiksel yöntemler uygulanarak elde edilmiş öznitelikler listelenmiştir.

Tablo 4.3. Özgün RF veri kümemizin tüm öznitelikleri

Öznitelik takma ad	Öznitelikler
AG_skw	AG'nin çarpıklık değerleri dizisi
AG_krts	AG'nin basıklık değerleri dizisi
AG_mn	AG'nin ortalama değerleri dizisi
AG_hmn	AG'nin harmonik ortalama değerleri dizisi
AG_gmn	AG'nin geometrik ortalama değerleri dizisi
AG_var	AG'nin varyans değerleri dizisi
AG_std	AG'nin standart sapma değerleri dizisi
AG_mdn	AG'nin medyan değerleri dizisi
AG_mdnL	AG'nin ortanca düşük değerleri dizisi
AG_mdnH	AG'nin ortanca yüksek değerleri dizisi
AG_mdnG	AG'nin medyan gruplandırılmış değerleri dizisi
AFa_skw	AFa'nın çarpıklık değerleri dizisi
AFa_krts	AFa'nın basıklık değerleri dizisi
AFa_mn	AFa'nın ortalama değerleri dizisi
AFa_var	AFa'nın varyans değerleri dizisi

AFa_std	AFa'nın standart sapma değerleri dizisi
AFa_mdn	AFa'nın medyan değerleri dizisi
AFr_skw	AFr'nin çarpıklık değerleri dizisi
AFr_krts	AFr'nin basıklık değerleri dizisi
AFr_mn	AFr'nin ortalama değerleri dizisi
AFr_var	AFr'nin varyans değerleri dizisi
AFr_std	AFr'nin standart sapma değerleri dizisi
AFr_mdn	AFr'nin medyan değerleri dizisi

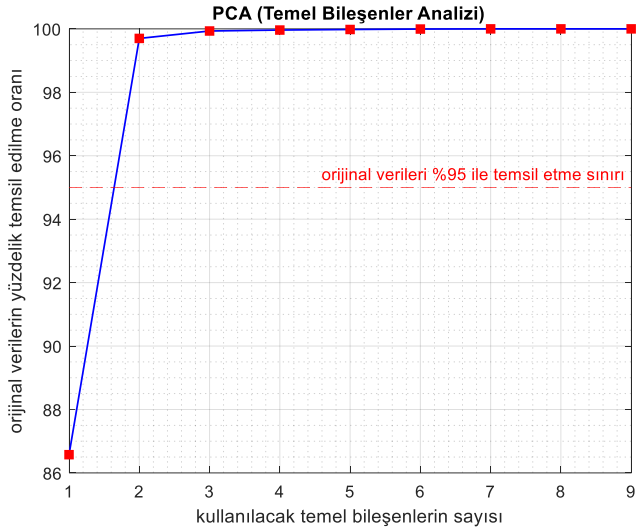
RF parmak izi veri toplama sistemiyle oluşturduğumuz veri kümesi %70 eğitim ve %30 test olmak üzere ayrılmıştır. Bu özgün RF öznitelikelerine ait veri kümesi Github üzerinden *https://github.com/HuseyinPARMAKSIZ/Own-IoT-RF-DS/blob/main/IoT-7-2103A.mat* adresinde paylaşılmaktadır. Toplam 368 öznitelik (16x23) içeren veri kümesine MRMR öznitelik seçim algoritması kullanılarak toplamda 136 öznitelik seçilmiştir. Literatürde yayınlanmış RF parmak izi çalışmalarından elde edilen örnek veri kümeleri ve bu çalışmada oluşturduğumuz veri kümesi Tablo 2.7'de yer almaktadır. Ayrıca sinyal yakalama işlemlerinde SDR'ler dışında çeşitli osiloskopların kullanıldığı da tabloda görülmektedir. Yine tabloda cihazların farklı iletişim teknolojilerini kullanarak iletişim kurduğu görülmektedir.

4.5. Temel Bileşenler Analizi (PCA)

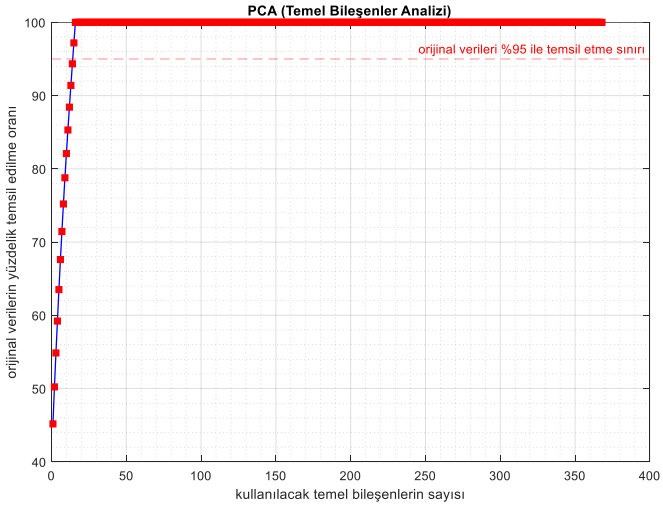
PCA; tanıma, sınıflandırma, görüntü sıkıştırma alanlarında kullanılan yararlı bir istatistiksel tekniktir. Ana amacı, yüksek boyutlu verilerde en yüksek varyans ile veri kümesini tutmaktır, ancak bunu yaparken boyut indirgemeyi sağlayan bir tekniktir. Fazla boyutlu verilerdeki genel özellikleri bularak boyut sayısının azaltılmasını, verinin sıkıştırılmasını sağlamaktadır. Boyut azalmasıyla bazı özelliklerin kaybedileceği kesindir fakat amaçlanan, bu kaybolan özelliklerin popülasyon hakkında çok az bilgi içeriyor olmasıdır. Bu yöntem, yüksek korelasyonlu değişkenleri bir araya getirerek verilerdeki en çok varyasyonu oluşturan "temel bileşenler" olarak adlandırılan daha az sayıda yapay değişken kümesi oluşturur. PCA verideki gerekli bilgileri ortaya çıkarmada oldukça etkili bir yöntemdir. PCA'in arkasında yatan temel mantık çok boyutlu bir veriyi, verideki temel özellikleri yakalayarak daha az sayıda değişkenle göstermektir (Köse vd., 2019).

JOA-VK'de 9 öznitelik (*Label, Mean, GMean, HMean, Median, MedianL, MedianH, MedianG, Variance, Stdev*) ve 4 farklı sınıf (0, 1, 2, 3) bulunmaktadır. Veri kümesi üzerinde PCA dönüşümü yapıldığında 2 bileşen seçerek, verilerin toplam varyansının yaklaşık % 99.6991796508535'sini korunabilmektedir. Tüm bileşenleri kullanmayarak sadece ana bileşenleri kullanmak istediğimiz için bu varyans oranı yeterli olacaktır. İlk bileşenin (PC1)

varyans oranı yaklaşık 0.865748787848751 etki etmektedir. Sırasıyla PC2= 0.131243008659784, PC3= 0.00233788025199250 varyans oranları ile etki etmektedir. Buradan yola çıkarak Şekil 4.5'te görüldüğü üzere, PC1+PC2 varyans oranı ~ %99.7 olarak veriyi temsil edeceğinden bu iki bileşenle veriyi temsil etmek yeterli olacaktır.



Şekil 4.5. JOA-VK üzerinde PCA analizi



Şekil 4.6. BVK üzerinde PCA analizi

Şekil 4.5 ve Şekil 4.6 karşılaştırıldığında %95 ve üzerinde verinin temsil edilebilmesi için 9 öznitelikli JOA-VS'den 2 bileşen, 368 öznitelikli BVS'den ise 15 bileşen kullanılması gerekmektedir.

4.6. MRMR ile Öznitelik Seçimi

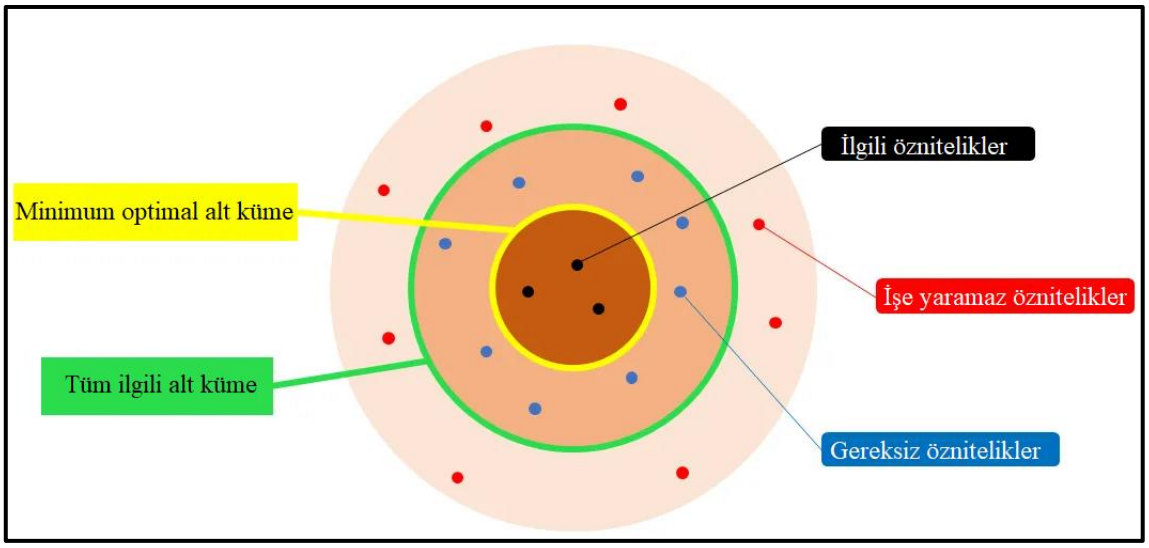
MRMR (Max-Relevance Min-Redundancy), makina öğrenimi ve örüntü tanıma alanında bir özellik seçme algoritmasıdır. MRMR algoritması, birbiriyle yüksek oranda ilişkili olmayan en alakalı öznitelikleri seçmeyi amaçlamaktadır. MRMR algoritması, öncelikle her bir özellik ile hedef sınıf arasındaki ortak bilgileri hesaplayarak çalışır. İki değişken arasındaki karşılıklı bilgi, aralarındaki bağımlılığı ölçer. Daha sonra, MRMR algoritması her özellik çifti arasındaki korelasyonu hesaplar. Son olarak, MRMR algoritması, hedef sınıfla yüksek karşılıklı bilgiye sahip ve diğer özelliklerle düşük korelasyona sahip öznitelikleri seçer. Amaç, verileri etkili bir şekilde temsil edebilen ve bir sınıflandırma algoritmasının başarımını iyileştirebilen bir özellik alt kümesi seçmektir. Algoritma 4.1'de MRMR'ın algoritması (Ramírez-Gallego vd., 2017) verilmiştir.

```
Girdi: adaylar, istenilenOznitelikSayisi
// adaylar başlangıç özellikleri kümesidir.
// istenilenOznitelikSayisi, seçilen özniteliklerin sayısıdır.
Çıktı: secilenOznitelikler // Seçilen öznitelikler kümesi.
1     for ozellikler fi in adaylar do
2     |     ilgi = karsilikliBilgi (fi, sinif);
3     |     fazlalik = 0;
4     |     for ozellikler fj in adaylar do
5       |     | fazlalik += karsilikliBilgi (fi, fj);
6     |     end for
7     |     mrmrDegerler[fi] = ilgi – fazlalık;
8     end for
9     secilenOznitelikler = sirala (mrmrDegerler).al(istenilenOznitelikSayisi);
```

Algoritma 4.1. MRMR Algoritması

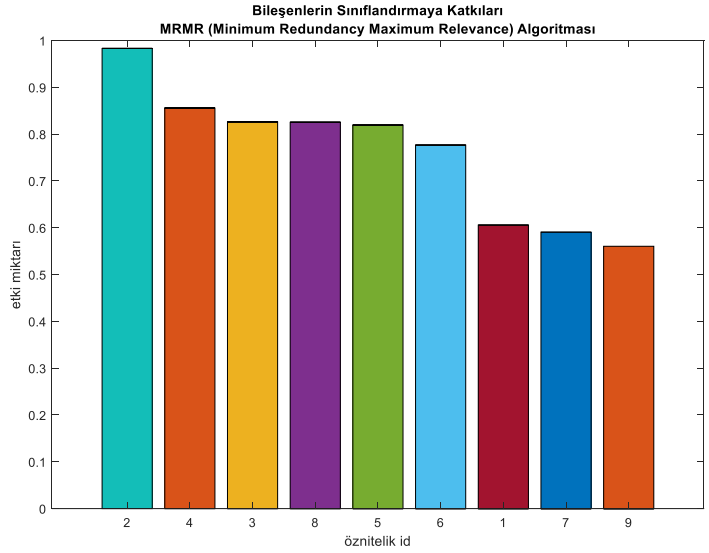
Kaynak: (Ramírez-Gallego vd., 2017)

Öznitelik seçim algoritmaları genel olarak iki (minimum-optimal ve tüm ilgili) kategoride sınıflandırılabilir. MRMR (minimum-optimal) özniteliklerin ilişkisini ve gereksizliğini dikkate alarak seçim yaparken, Boruta (tüm ilgili), rastgele orman algoritması kullanarak özniteliklerin önem sıralamasını belirlemektedir. Öznitelik seçimi Şekil 4.7'deki görsel gibi dart oynamaya benzetilmektedir. Dart oynamada olduğu gibi, öznitelik seçimi sürecinde de hedef, maksimum bilgi veya başarım elde etmek için doğru öznitelikleri seçmektir. Öznitelikler arasında ilişkileri değerlendirmek, özniteliklerin önem sıralamasını belirlemek ve gereksiz öznitelikleri elemek önemlidir. Bu nedenle, öznitelik seçimi süreci, dart oynamaya benzetilir çünkü doğru hedefe odaklanma ve sınırlı kaynakları etkili bir şekilde kullanma fikrine dayanmaktadır.

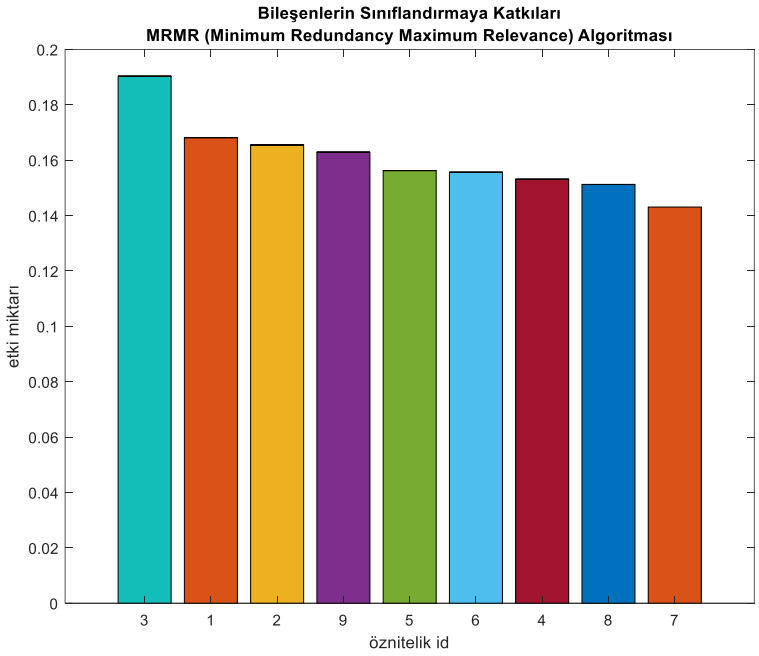


Şekil 4.7. Öznitelik seçimi ve dart ile ilişkilendirimi

Sınıflandırmada öznitelikler önemlidir. Sınıflandırıcının doğruluğunu artırmak ve sistem kaynaklarının etkin kullanılması için çeşitli öznitelik indirgeme algoritmaları mevcuttur. JOA-VK'de MRMR algoritması ile en etkili öznitelikler Şekil 4.8'de bar olarak etki miktarına göre sıralı hali ile gösterilmektedir. Şekil 4.9'da ise BVK'deki en etkili ilk 9 öznitelik verilmektedir.



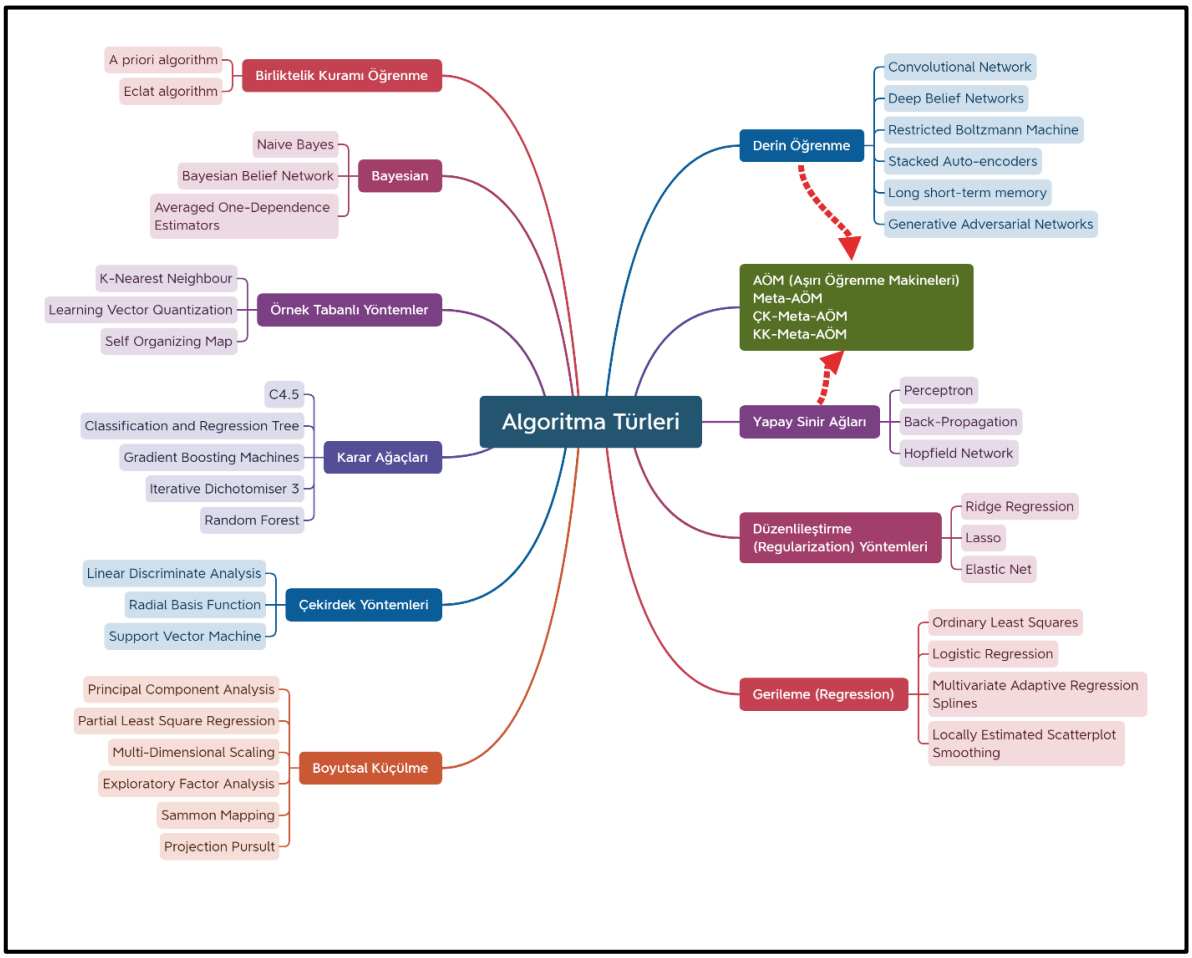
Şekil 4.8. Özniteliklerin sınıflandırmaya etkisi (9 öznitelikli JOA-VK).



Şekil 4.9. MRMR algoritması ile en etkili 9 öznitelik (368 öznitelikli BVK).

5. GRUP AÖM YAPILARI İLE RF PARMAK İZİ TABANLI IoT CİHAZ TANIMLAMA

Giriş bölümünde RF parmak izi tabanlı cihaz tanıma çalışmaları özatlenmiş ve Tablo 1.2 ile literatürde RF parmak izi çalışmalarında kullanılan özellikler ve sınıflandırma algoritmalarını sunulmuştur. Tablodan da görüleceği üzere bu alanda AÖM tabanlı sınıflandırıcıların kullanılması henüz mevcut değildir. Bu tez çalışmasında cihazları ayıt etmek amaçlı grup AÖM yapıları kullanılmıştır. AÖM'ler Şekil 5.1'de görüldüğü üzere derin öğrenme ve yapay sinir ağlarını birleştirmektedir.

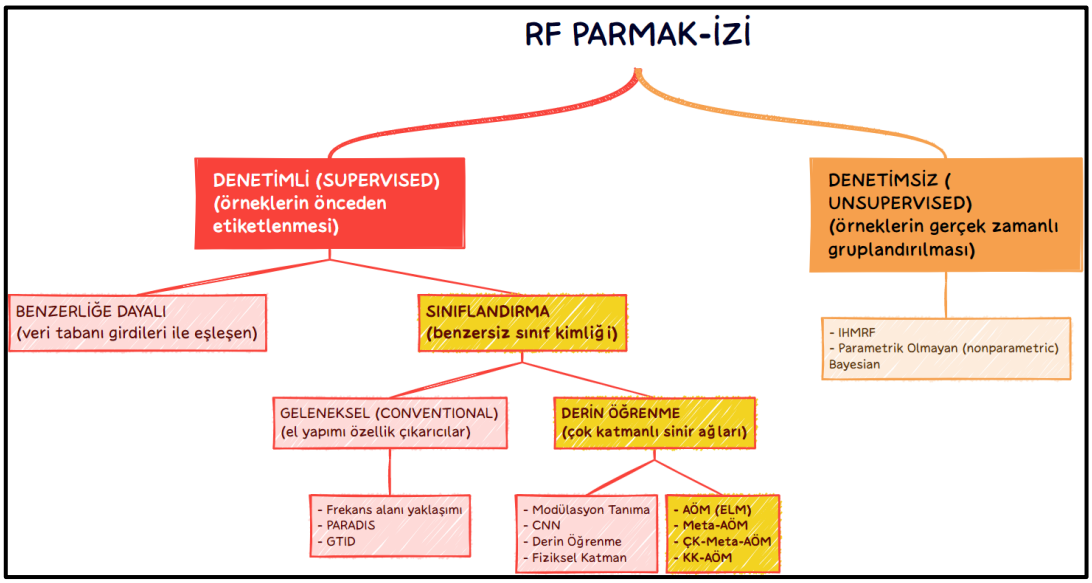


Şekil 5.1. Literatürdeki algoritma türleri

5.1. Sınıflandırıcı Algoritma Çalışmaları

Aşırı öğrenme ağları ile sınıflandırma işlemi IoT/Wi-Fi cihazlarından MEC tarafından yakaladığımız sinyallerden elde edeceğimiz öznitelikler ile donanım kimliklendirme ve model eğitimi yapılacaktır. Şekil 5.2'de kimliklendirme için kullanılan yöntemlerin literatürde mevcutlarına göre durumu verilmiştir. Bu noktada kimliklendirme yapılacak donanımın ürettiği

işareti elde etmeye yarayacak olan ve MEC'te yer alacak olan alıcı özelliklerine bağlı sınıflandırma başarım değişimleri söz konusu olabilmektedir. Bu durumun üstesinden gelmek adına gerekli öğrenme teknikleri ile alıcı bağımsız bir sistem geliştirilmiştir.



Şekil 5.2. Literatürdeki RF parmak izi tanıma yöntemleri ve AÖM'nin konumu

Diğer yandan sistemin kimliklendirme yapabileceği cihaz sayısının limitlerini belirlemek ve eğitim verisi oluşturmak için AÖM kullanımı değerlendirilmiştir. Sonuç olarak tezin temelindeki kimliklendirme süreci için grup AÖM öğrenme güncel teknik ve yaklaşımlar kullanılmıştır.

5.1.1. AÖM

Pek çok mühendislik ve bilim problemi sinir ağları kullanılarak çözülür ve bu ağları eğitmek için genellikle yinelemeli algoritmalar kullanılır. İleri beslemeli sinir ağlarında, ağ parametrelerini (eşikler ve ağırlıklar) belirlemek için yinelemeli, türev tabanlı algoritmalar kullanılır. Türev tabanlı yinelemeli algoritmaların eğitim süresinin yavaş olması sonucu yeni arayışlar başlamıştır. Tek gizli katmanlı ileri beslemeli ağlar (SLFN) için tasarlanmış bir öğrenme algoritması olan AÖM, bu yavaşlığın üstesinden gelir. 2006 yılında Huang ve diğerleri tarafından önerilmiştir (G.-B. Huang vd., 2006).

AÖM bir makina öğrenme algoritmasıdır ve özellikle hızlı öğrenme ve yüksek doğruluk gerektiren uygulamalarda kullanılabilir. AÖM, giriş ağırlıkları rastgele atanan çıkış ağırlıkları ise analitik olarak hesaplanan SLFN bir YSA modelinin özelliştirilmiş biçimidir (G.-B. Huang ve Siew, 2004; G.-B. Huang vd., 2004, 2006). AÖM'de gizli katman ile çıktı katmanı

arasındaki ağırlıklar tek seferde doğrusal bir model ile analitik ve hızlıca belirlenmektedir. Bu modelde giriş katmanındaki nöronlara ait ağırlıklar ve gizli katmandaki nöronlara ait eşik değerleri rastgele üretilirken gizli katmandaki çıkış ağırlıkları analitik olarak hesaplanmaktadır (Tang vd., 2014). AÖM'de gizli katmanda sigmoid, sinüs ve Guassian v.d. aktivasyon fonksiyonları kullanılırken çıkış katmanında doğrusal fonksiyon kullanılmaktadır.

AÖM, eğitim süresi açısından önemli bir üstünlüğe sahipken, genelleme kapasitesi açısından da başarımı yüksek seviyelere ulaştırılmıştır. Çok sayıda gömülü nöron nedeniyle genelleme yapmayı öğrenebilir. Nöron sayısı, eğitim örneklerinin sayısından (L>N) daha büyük olduğunda, doğrusal sistemin ($\boldsymbol{H\beta} = \mathbf{T}$) sıfır hatayla birçok çözümü olacağı açıktır ve her durum fazla uydurma ile sonuçlanır. SLFN'yi L<N ile eğitmek için (G.-B. Huang vd., 2006), eşitlik (5.1)'i sağlayan bir çözüm bulunur. Eşitlik (5.2)'de verilen maliyet fonksiyonunu en aza indirmek için eğitim yapılır. Bu süreç eşitlik (5.3)'de verilen koşulu sağlayan belirli $\hat{\mathrm{w}}_\mathrm{i}, \hat{b}_i, \hat{\beta} (i = 1, \dots, L)$ 'yı bularak sonlandırılmalıdır.

$$|| \boldsymbol{H\beta} - \mathbf{T} || < \varepsilon \tag{5.1}$$

$$C = \sum_{j=1}^{N} \left[\sum_{i=1}^{L} \beta_i G(w_i, b_i, x_j) - t_j \right]^2, \tag{5.2}$$

$$|| \boldsymbol{H}(\hat{\mathbf{w}}_\mathbf{1}, \dots, \hat{\mathbf{w}}_\mathbf{L}, \hat{b}_1, \dots, \hat{b}_L)\hat{\beta} - \boldsymbol{T} || = \frac{min}{\hat{\mathrm{w}}_\mathrm{i}, \hat{b}_i, \beta} || \boldsymbol{H}(\mathbf{w}_\mathbf{1}, \dots, \mathbf{w}_\mathbf{L}, b_1, \dots, b_L)\beta - \boldsymbol{T} ||. \tag{5.3}$$

Giriş ağırlıklarının ve gizli katman sapmalarının ayarlanmasını gerektiren geleneksel fonksiyon yaklaşım teorilerinin aksine, giriş ağırlıkları ve gizli katman sapmaları, (G.-B. Huang vd., 2006)'da titizlikle gösterildiği gibi, yalnızca aktivasyon fonksiyonu sonsuz derecede türevlenebilir ise rastgele atanabilir. Sabit girdi ağırlıkları ($\mathbf{w_i}$) ve nöronların bias değerleri ($\mathbf{b_i}$) ile bir SLFN'yi eğitmek için, yalnızca belirli çıktı ağırlıklarını ($\boldsymbol{\beta}$)'yı bulmak için eşitlik (5.4) kullanılmaktadır.

$$|| \boldsymbol{H\hat{\beta}} - \boldsymbol{T} || = \frac{min}{\beta} || \boldsymbol{H\beta} - \boldsymbol{T} || \tag{5.4}$$

L<N, AÖM, eşitlik (4.4)'te $\hat{\boldsymbol{\beta}}$ 'yı belirlemeye eşdeğer olan maliyet fonksiyonunu en aza indirerek $\boldsymbol{\beta}$ çıkış ağırlığını öğrenir. AÖM eşitlik (5.5) ile $\boldsymbol{\beta}$ 'yı belirler.

$$\boldsymbol{\beta} = \mathbf{H}^{\dagger}\mathbf{T} \tag{5.5}$$

$\mathbf{H}^{\dagger}$, H matrisinin Moore-Penrose genelleştirilmiş tersidir (Rao ve Mitra, 1972). Eşitlik (5.5)'de tanımlanan $\hat{\boldsymbol{\beta}}$ çözümü, lineer sistemin ($\boldsymbol{H\beta} - \boldsymbol{T}$) en küçük kareler çözümlerinden biridir ve tüm çözümler arasında en düşük norma sahiptir. (G.-B. Huang vd., 2006)' ya göre, $\widehat{\boldsymbol{\beta}}$ yalnızca eğitim hatasını en aza indirmekle kalmaz, aynı zamanda en küçük ağırlık büyüklüğüne de sahiptir. Sonuç olarak $\widehat{\boldsymbol{\beta}}$, diğer tüm en küçük kareler çözümleri arasında en iyi genelleme yapabilenidir. AÖM'de ortogonal izdüşüm yöntemi etkin bir şekilde kullanılabilir: $\mathbf{H}^{\mathrm{T}}\boldsymbol{H}$ değeri tekilse (singular) $\mathbf{H}^{\dagger} = (\mathbf{H}^{\mathrm{T}}\boldsymbol{H})^{-1}\mathbf{H}^{\mathrm{T}}$, $\mathbf{H}\mathbf{H}^{\mathrm{T}}$ değeri tekil değilse (nonsingular) $\mathbf{H}^{\dagger} = \mathbf{H}^{\mathrm{T}}(\mathbf{H}\mathbf{H}^{\mathrm{T}})^{-1}$ (G. -B. Huang vd., 2011). AÖM'nin yapısal ve eğitim adımları, Algoritma 5.1'de özetlenmiştir:

Girdi: $\mathcal{N} = \{(\mathbf{x}_i, t_i) \mid \mathbf{x}_i \in \mathbb{R}^d, t_i \in \mathbb{R}, i = 1, \ldots, N\}$ // Eğitim kümesi
$G(\mathrm{w}_i, b_i, \mathrm{x})$ // Gizli düğüm işlevi
L // Gizli düğüm sayısı
Çıktı: β // Çıktı ağırlık vektörü

// ***Adım 1***, gizli düğüm parametrelerini rastgele oluştur. $(\mathrm{w}_i, b_i), i = 1, \ldots, L$
for $i = 1{:}L$ **do**
    w_i, b_i rastgele ata
end
// ***Adım 2***, Gizli katman çıkış matrisi $\mathbf{H}'$yi hesaplama.
for $i = 1{:}L$ **do**
    for $j = 1{:}N$ **do**
        $\mathrm{H}(i,j) = G(\mathrm{w}_i, b_i, \mathrm{x}_j)$;
    end
 end
// ***Adım 3***, Çıkış ağırlık vektörü β'yı hesaplama.
$\beta = \mathbf{H}^{\dagger}\mathrm{T}$

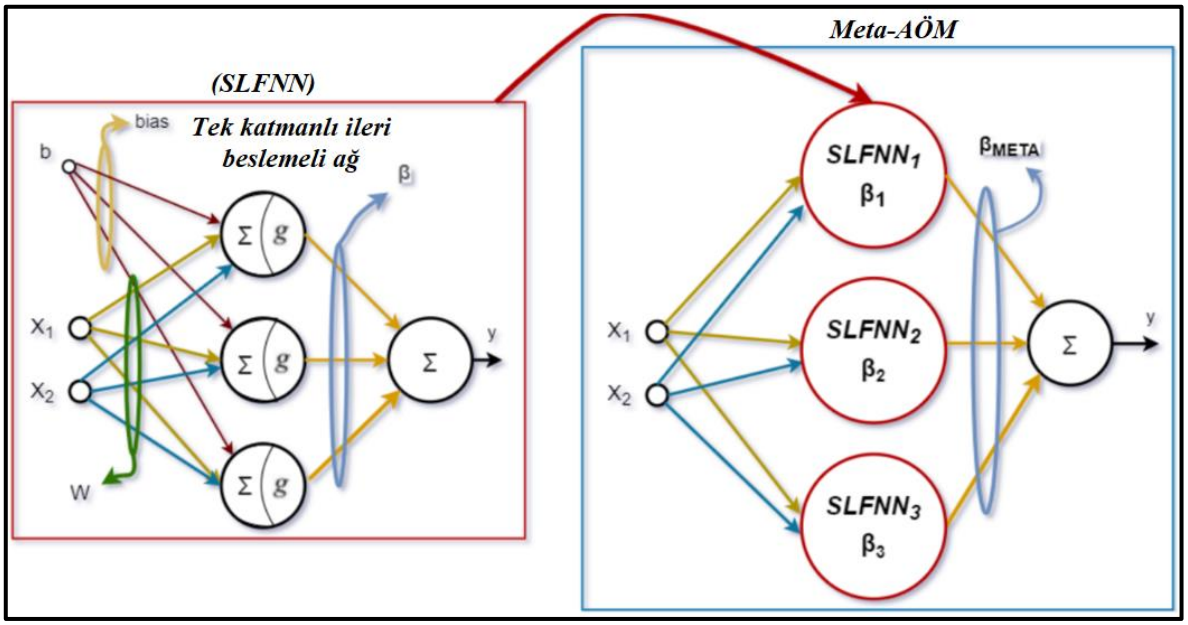
Algoritma 5.1. Çok giriş-tek çıkış modelleme için AÖM algoritması

Kaynak: (G.-B. Huang vd., 2006).

Bu tezde sınıflayıcı olarak AÖM tabanlı sınıflayıcılar kullanılmıştır. Bu ağ yapılarına adını veren en belirgin özelliği, çok hızlı öğrenme sürecini temin etmeleridir. 2004'den itibaren AÖM tabanlı ağlar zamanla çeşitlenmiş ve birçok ağ yapısı geliştirilmiştir. Bu geliştirmeler genellikle mevcut sinir ağları ve onların mimarileri ekseninde olmuştur. Bu ağlar içinde sınıflandırma başarımları açısından dikkate değer olanlar Meta-AÖM (Liao ve Feng, 2014) ve yakın geçmişte geliştirilen ÇK-AÖM (Tang vd., 2015) ve ÇK-KAÖM (Wong vd., 2016) adlı çok katmanlı AÖM'lerdir. Şekil 5.3'te klasik AÖM ve Meta-AÖM yapıları verilmiştir. Klasik

AÖM ve çok katmanlı AÖM ağları hakkında gerekli bilgiye yukarıda atıf yapılan çalışmaların yanı sıra (Bakırcı, 2019) ve (Karakuzu, 2020)'dan ulaşılabilir. AÖM türlerinin sınıflandırma karşılaştırmalarında, düzenleme faktörü λ bu çalışma kapsamında eşitlik (5.6)'daki formülasyonla belirlenmektedir. Düzenleme faktörü genellikle ampirik olarak belirlenir ve soruna ya da incelenen veri kümesine bağlı olarak değişmektedir. Düzenleme faktörü determinantın sıfır olmasını önlemektedir. X ise eğitim kümesindeki veri kümesini temsil etmektedir.

$$\lambda = \max(eig(\boldsymbol{X'X})) \tag{5.6}$$



Şekil 5.3. Klasik AÖM(sol) ve META-AÖM (sağ) ağ yapıları

Çalışma çerçevesinde iyi bir genelleme yeteneğini gözlediğimiz Meta-AÖM yapısından esinlenerek ÇK-Meta-AÖM adını verdiğimiz yeni bir ağ yapısı geliştirerek ve sınıflandırıcı olarak kullanılmıştır. Bu ağ yapısı, Şekil 5.3'ün sağ tarafında verilen yapıda SLFNN'ler yerine ÇK-AÖM ve/veya Kısıtlı-AÖM ağ yapılarını ve öğrenme yaklaşımlarınının kullanımı olarak özetlenebilir.

5.1.2. Kısıtlı AÖM'ler

Örnek dağılımına dayalı olarak gizli nöronların parametrelerini rastgele seçmek için "kısıtlı aşırı öğrenme makinaları" (K-AÖM'ler) adı verilen yeni atama yöntemleri önerilmiştir (W. Zhu vd., 2015). AÖM'deki gizli düğümlerin parametrelerini (bağlantı ağırlık ve eşiklerini) tamamen rastgele seçilmesiyle karşılaştırıldığında, K-AÖM'ler orijinal örnek vektörlerin bazı

temel kombinasyonlarını içeren kısıtlı vektör uzayından parametre ataması yaparlar. Deneysel sonuçlar, K-AÖM'lerin geleneksel AÖM, SVM ve diğer bazı ilgili yöntemlerden daha iyi genelleme yeteneğine sahip olduğunu göstermektedir. Ek olarak, K-AÖM 'ler, AÖM ile benzer bir öğrenme hızına sahiptir. Geleneksel AÖM ağ yapısında ağ giriş parametrelerinin atanması için örnek vektörlerin basit doğrusal kombinasyonunu kullanma fikriyle ortaya atılan K-AÖM'ler şunlardır: Constrained Difference Extreme Learning Machine (CD-ELM), Sample Extreme Learning Machine (SELM), Constrained Sum Extreme Learning Machine (CS-ELM), Random Sum Extreme Learning Machine (RSELM) ve Constrained Mixed Extreme Learning Machine (CM-ELM).

K-AÖM kodları *https://github.com/HuseyinPARMAKSIZ/Constrained-ELMs* adresinde verilmektedir.

5.1.3. ÇK-AÖM

ÇK-AÖM yapısında tek katmanlı AÖM yerine çok katmanlı AÖM katmanları bulunmaktadır. Bu yapıda, son katman haricinde tüm katmanlar otomatik kodlayıcılardır (AE). $\mathbf{H}\mathbf{H}^T$ tekil olmadığında, $\mathbf{H}$ matrisinin Moore-Penrose tersi $\mathbf{H}^T(\mathbf{H}\mathbf{H}^T)^{-1}$ olarak da gösterilebilir. Sırt regresyonu teorisi kullanıldığında, $\mathbf{H}\mathbf{H}^T$ matrisinin diyagonal elemanlarına ($\frac{\mathbf{I}}{\lambda}$) değerleri eklenir. ÇK-AÖM yapısının bir katman için öğrenme denklemi Eşitlik (5.7)'de verilmektedir.

$$\beta = \mathrm{H}^T\left(\frac{\mathrm{I}}{\lambda} + \mathrm{H}\mathrm{H}^T\right)^{-1}\mathrm{T} \tag{5.7}$$

ÇK-AÖM yapısında her gizli katman için temsili girişler bulunmaktadır. Katman i için temsili giriş d adet harici giriş kullanıldığında $\mathbf{X}^{(i)} = \left[\mathbf{x}_1^{(i)}, \ldots, \mathbf{x}_d^{(i)}\right]$ olarak ifade edilebilir. Katman i için transformasyon matrisi $\boldsymbol{\beta}^{(i)} = \left[\boldsymbol{\beta}_1^{(i)}, \ldots, \boldsymbol{\beta}_d^{(i)}\right]$'dir. Temsili giriş $\boldsymbol{X}^{(i)} = \boldsymbol{H}^{(i)}\boldsymbol{\beta}^{(i)}$'dır. Temsili giriş kullanılarak $\boldsymbol{\beta}^{(i)}$ Eşitlik (5.8) kullanılarak hesaplanmaktadır.

$$\boldsymbol{\beta}^{(i)} = \boldsymbol{H}^{(i)^T}\left(\frac{\mathrm{I}}{\lambda} + \boldsymbol{H}^{(i)}\boldsymbol{H}^{(i)^T}\right)^{-1}\boldsymbol{X}^{(i)} \tag{5.8}$$

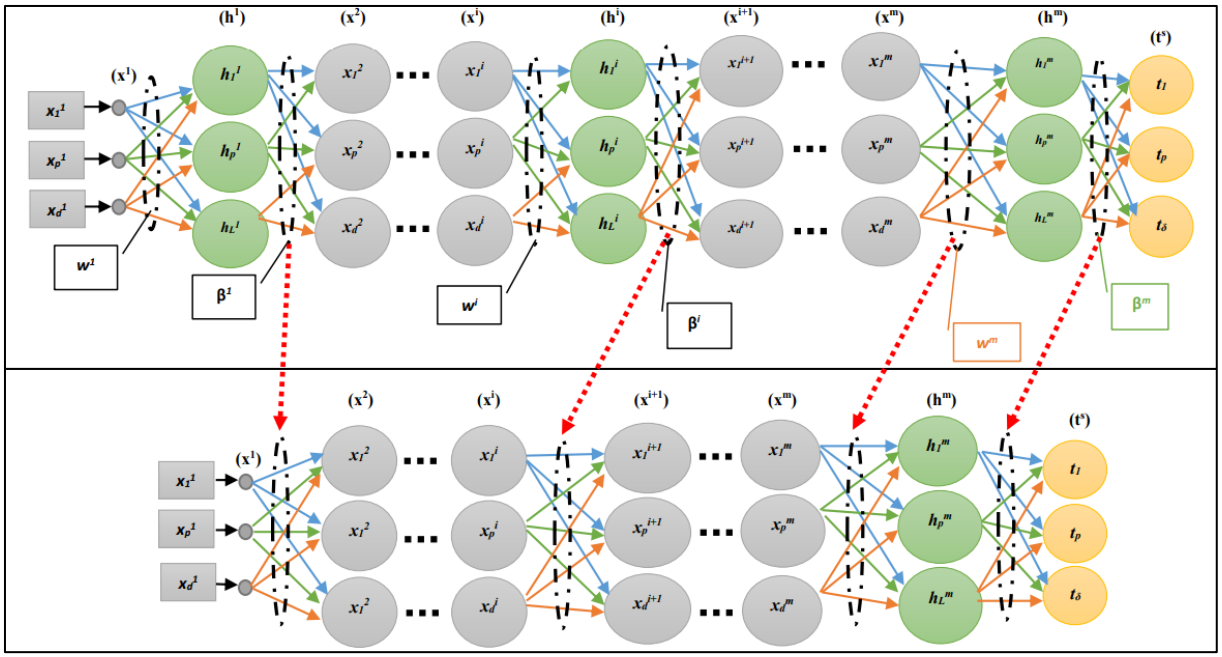
M katman için son katmanın çıkış matrisi $\boldsymbol{H}^{(M)}$ olarak adlandırılır. Bu çıkış matrisini kullanarak son katmanın çıkış ağırlık matrisi $\boldsymbol{\beta}^{(M)}$ Eşitlik (5.9) ile hesaplanmaktadır.

$$\boldsymbol{\beta}^{(M)} = \left(\mathbf{H}^{(M)}\right)^T\left(\frac{\mathbf{I}}{\lambda} + \mathbf{H}^{(M)}\left(\mathbf{H}^{(M)}\right)^T\right)^{-1}\mathrm{T} \tag{5.9}$$

ÇK-AÖM'nin eğitim aşamasında öğrenilen $\boldsymbol{\beta}$, test aşamasında kullanılmak üzere saklanmalıdır. Son olarak, test aşamasında, eğitim aşamasının son katmanının ağırlık parametreleri kullanılır (Kale ve Karakuzu, 2022). Bu durumda, I birim matrisi temsil ederken, $\boldsymbol{\lambda}$ yapısal ve deneysel riski ayarlamak için kullanılan düzenleme parametresini temsil eder. Şekil 5.4'de gösterildiği gibi, AÖM ve AÖM-AE birleştirilerek çok katmanlı AÖM oluşturulur, bu da birden fazla gizli katmana sahiptir (Kasun vd., 2013).

ÇK-AÖM'in en önemli özelliklerinden bazıları şunlardır (Kaur vd., 2023):

- *Yüksek Hız:* ÇK-AÖM, hızlı bir şekilde eğitim ve tahmin yapabilme yeteneğine sahiptir. Büyük veri kümeleriyle bile etkili bir şekilde çalışabilir.
- *İyi Genelleştirme:* ÇK-AÖM, genelleştirme yeteneği yüksek olan bir modeldir. Eğitim verilerinde iyi performans göstermesinin yanı sıra, yeni verilere de iyi uyarlanabilir.
- *Az Hiperparametre:* ÇK-AÖM, diğer bazı yapay sinir ağı modellerine göre daha az hiperparametreye sahiptir. Bu, modelin yapılandırılmasını ve uyarlanmasını kolaylaştırır.
- *Ölçeklenebilirlik:* ÇK-AÖM, ölçeklenebilir bir yapıya sahiptir. Veri kümesinin boyutu arttıkça, modelin performansı ve hızı düşmez.
- *İyi Sonuçlar:* ÇK-AÖM, birçok uygulama alanında iyi sonuçlar veren bir modeldir. Sınıflandırma, regresyon, görüntü işleme ve keşifçi veri analizi gibi birçok alanda başarılı sonuçlar elde edebilir.



Şekil 5.4. ÇK-AÖM'nin eğitim sırasında (üst) ve eğitim sonrasında (alt) kullanım mimarisi (d harici giriş ve δ harici çıkışlı m katmanlı)

5.1.4. Meta-AÖM

Meta-AÖM bir makina öğrenme algoritmasıdır ve asıl AÖM algoritmasının bir geliştirilmiş versiyonudur. Meta-AÖM, birçok tek katmanlı AÖM ağının birleşiminden oluşan bir topluluk AÖM ağ yapısıdır. Meta-AÖM, AÖM'e göre daha fazla verimlilik ve güvenilirlik sunarak daha iyi sonuçlar vermektedir Ancak, doğal olarak AÖM'ye göre daha fazla süre ve kaynak gerektirmektedir. Meta-AÖM, literatürde regresyon uygulamalarında yaygın olarak kullanılmaktadır. RF sinyal çalışmalarında henüz aktif olarak kullanılmamıştır. Prof. Dr. Cihan KARAKUZU ve Prof. Guang-Bin HUANG'ın bu alandaki örnek kodları tezimizde kullanılmıştır.

Meta-AÖM hiyerarşik bir öğrenme modelidir. AÖM'den farklı olarak Meta-AÖM, tüm veri kümesini ayrık alt kümelere ayırır, alt kümeler üzerinde tahmin ediciler (temel AÖM'ler) üretir ve tahmin edici ağırlıklarını analitik olarak hesaplar. Meta-AÖM, maliyet fonksiyonunu en aza indirmek için eşitlik (5.10)'u kullanır.

$$J = \sum_{i=1}^{N} \left[\sum_{m=1}^{M} \beta_m \text{AÖM}_m(\mathbf{x}_i) - t_i \right]^2 \tag{5.10}$$

Burada, N, eğitim verilerinin sayısını, M ise Meta-AÖM modelindeki temel AÖM'lerin sayısını belirtir, $\text{AÖM}_m(\mathbf{x}_i)$, belirli bir $\mathbf{x}_i$ girişi için m'inci temel AÖM'nin çıktısını belirtir ve β_m, m'inci temel AÖM için çıktı ağırlık matrisini gösterir. Şekil 5.5'te Meta-AÖM ağ mimarisi gösterilmektedir. Algoritma 5.2'de Meta-AÖM'nin eğitim algoritması verilmektedir. Meta-AÖM algoritması AÖM tabanlı iki aşamalı öğrenme algoritmasından oluşmaktadır. Meta-AÖM algoritması, Adım 1'de verileri M ayrık alt kümeye böler ve ardından her bir alt kümeyi kullanarak temel AÖM'leri eğitir. Aşama 2, tüm eğitim verileriyle birlikte Aşama 1'de elde edilen önceden eğitilmiş temel AÖM'leri kullanarak bir üst AÖM'nin eğitimini içermektedir.

Girdi: $\mathcal{N} = \{(\mathbf{x}_i, t_i) \mid \mathbf{x}_i \in \mathbb{R}^d, t_i \in \mathbb{R}, i = 1, \dots, N\}$ // Eğitim kümesi
M // 1. Kısımda AÖM'lerin sayısı
Çıktı: β // 2. Kısımda çıktı ağırlık vektörü

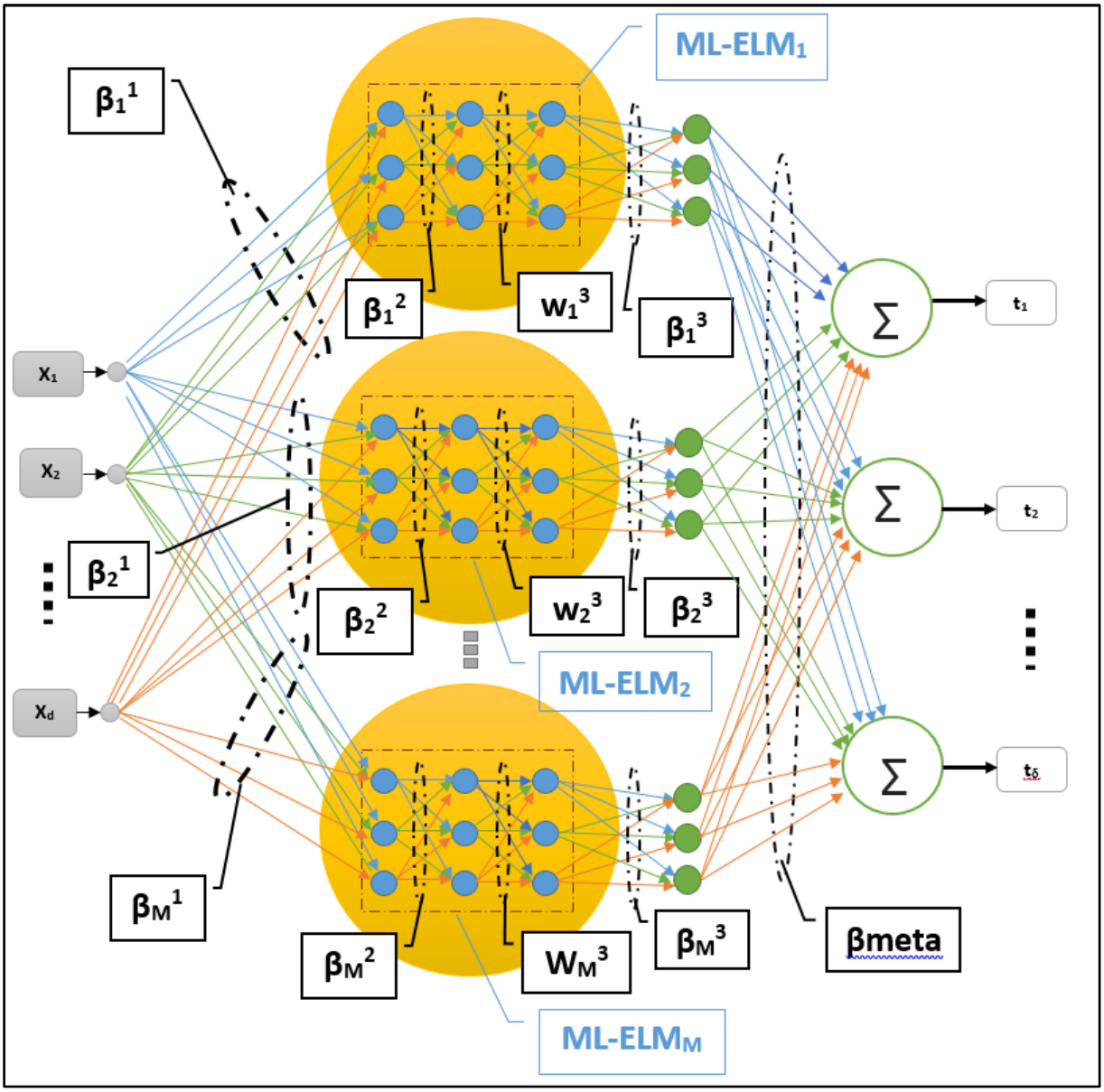
// ***Kısım 1:***
// ***Adım 1,*** tüm eğitim veri kümesini N/M 'ye yakın boyutta M alt kümeye bölün.
$S = \{S_i \mid S_i \subseteq \mathcal{N}, \cup_{i=1}^{M} S_i = \mathcal{N}, S_i \cap S_j = \emptyset, i \neq j,\ i, j = 1, \dots, M\}$
Adım 2, her temel AÖM'yi alt kümelerden biri üzerinden ayrı ayrı eğitin.
for each $S_i \in S$ **do**
| AÖM β_j 'yi S_j 'de öğrenir.
end
// ***Kısım 2:***
Adım 1, gizli katman çıkış matrisi **H** 'yi hesaplayın
// β_j j 'inci temel AÖM'nin çıktı ağırlık vektörüdür.
for $j = 1{:}M$ **do**
| **for** $i = 1{:}N$ **do**
| | $\mathrm{H}(i, j) = A\ddot{\mathrm{O}}M_j(\mathrm{x}_i) = h_j(\mathrm{x}_i) . \beta_j$
| **end**
end
// ***Adım 2,*** çıkış ağırlık vektörü $\boldsymbol{\beta}$ 'yı hesaplayın.
$\boldsymbol{\beta} = \mathbf{H}^{\dagger}\mathbf{T}$

Algoritma 5.2. Meta-AÖM eğitim algoritması.

5.1.5. ÇK-Meta-AÖM

ÇK-AÖM bir makina öğrenme algoritmasıdır ve AÖM algoritmasının birden fazla gizli katman içeren bir versiyonudur. ÇK-AÖM, çoklu katman yapısı ile daha iyi başarım ve daha

karmaşık problemleri çözme imkanı sağlamaktadır. Ancak, AÖM'ye göre daha fazla zaman ve kaynak gerektirebilir. ÇK-AÖM hiyerarşik AÖM olarak tanımlanan çok katmanlı bir AÖM yapısıdır (Tang vd., 2015). Bu yapıda birbirinden bağımsız temsili ve final öğrenme olmak üzere toplamda iki farklı prosedür mevcuttur. Sadece giriş örnekleri ile katman katman ilerleyerek son katmana kadar temsili öğrenmenin işletilme süreci vardır, bu süreç (hiyerarşik öğrenme) özellik çıkarımı olarak düşünülebilir. Son katmanda, hiyerarşik olarak işlenmiş giriş ve çıkış örnekleriyle klasik AÖM yöntemi uygulanarak final öğrenme gerçekleştirilmektedir. M katmanlı, d harici giriş ve δ harici çıkışlı bir ÇK-AÖM'nin yapısı Şekil 5.4'te verilmektedir. Şekilde, i katman sayısı ve j ise o katmandaki hücre sayısını belirtmektedir. Son katman hariç diğer katmanlar oto-kodlayıcı olarak ifade edilmektedir. Ağdaki her katman, ortogonal rastgele atanmış kendi giriş bağlantı ve eşik parametrelerine sahiptir. Katman çıkış matrisi hesapları yapıldıktan sonra oto-kodlayıcı katmanlar için Moore-Penrose genelleştirilmiş ters ile kararlılığı arttırmak adına λ düzenleme faktörü eklenerek dönüşüm matrisi belirlenmektedir. Son katman için bu hesaplama, istenen çıkış örnek matrisi ile yapılmaktadır. Şekil 5.6'da ÇK-Meta-AÖM yapısı verilmiştir.



Şekil 5.5. ÇK-Meta-AÖM yapısı

Algoritma 5.3'te Meta-AÖM sınıflandırı algoritmasının temel AÖM yapıları yerine ÇK-AÖM yapıları kullanılarak geliştirdiğimiz ÇK-Meta-AÖM algoritmasının kaba kodu verilmiştir.

```
1       // MRMR öznitelik seçimi yapılır.
2       // Sınıflandırma için eğitim ve test veri kümelerinin düzenlenmesi
3       |       Her bir örneğin hangi sınıfa ait olduğunu belirleyen etiketleme işlemi
yapılır.
4       // Alt ÇK-AÖM'ler (grup) için eğitim döngüsü başlar:
```

5 | ***Her bir ÇK-AÖM grubu için aşağıdaki adımlar tekrarlanır:***

5 | | Otomatik kodlayıcılar için temsil öğrenme yapılır.

6 | | Her bir katman için gizli düğümlerin giriş ağırlıkları ve hücre eşikleri atanır.

7 | | Aktivasyon fonksiyonu kullanılarak gizli katman çıktıları hesaplanır.

8 | | Beta çıkış ağırlıkları hesaplanır

9 | | Bir sonraki katmanın temsili girişi belirlenir

10 | ***Temel ÇK-AÖM'lerin son katmanının eğitimi yapılır:***

11 | | Son katman düğümlerinin giriş bağlantı ağırlıkları ve hücre eşikleri atanır.

12 | | Aktivasyon fonksiyonu kullanılarak katman çıktıları hesaplanır.

13 | | Beta çıkış ağırlıkları hesaplanır.

14 | | Eğitilmiş temel ÇK-AÖM'lerin çıktıları bulunur.

15 ***// Meta-AÖM eğitimi yapılır ve Beta_Meta parametreleri bulunur.***

16 | ***Her bir ÇK-AÖM grubu için aşağıdaki adımlar tekrarlanır:***

17 | | Oto-kodalama katmanlarına giriş verileri uygulanır.

18 | | Son katmanın çıktıları hesaplanır ve H_Meta'ya eklenir.

for $j = 1{:}M$ **do**

| **for** $i = 1{:}N$ **do**

| | $\mathrm{H\_Meta}(i,j) = ÇK - AÖM_j(\mathrm{x}_i) = h_j(\mathrm{x}_i).\beta_j$

| **end**

end

19 ***// Beta_Meta hesaplanır.***

$$\boldsymbol{\beta\_Meta} = \mathbf{H\_Meta}^{\dagger}\mathbf{T}$$

20 ***// ÇK-Meta-ÇKAÖM testi yapılır***

21 | ***Test veri kümesi için aşağıdaki adımlar tekrarlanır:***

22 | | Oto-kodlama katmanlarına giriş verileri uygulanır.

23 | | Son katmanın çıktıları hesaplanır ve H_Meta_t'ye eklenir.

24 ***// Ytest=H_Meta_t×Beta_Meta hesaplanır.***

Algoritma 5.3. ÇK-Meta-AÖM sınıflandırma algoritmasının kaba kodu.

5.1.6. KK-Meta-AÖM

KK-Meta-AÖM (Kısıtlı Karma Meta-AÖM), Meta-AÖM sınıflandırıcı algoritmasının başlangıç parametrelerinin atanması sürecinde Kısıtlı (Constrained) AÖM'lerden Kısıtlı Karma (Constrained Mixed) uygulanması ile geliştirdiğimiz algoritma yapısıdır.

AÖM, rastgele çok sayıda gizli düğüm oluşturarak genellikle istenen performansı elde eder. Gerçek dünya uygulamalarında bu, test sürecinde zaman kaybına yol açar. AÖM'nin bu dezavantajını avantaja çevirmek için aşağıdaki yaklaşımlar kullanılmaktadır:

- Gizli katman düğümlerini dinamik olarak ekleme (çevrimiçi artımlı öğrenme yöntemlerini kullanarak) (Lan vd., 2009; Q.-Y. Zhu vd., 2005).
- Aday gizli katman düğümlerinin seçilmesi (budama yöntemleri kullanılarak) (Rong vd., 2008).
- AÖM'de giriş katmanından gizli katmana ağırlıkları güncellemek için gradyan tabanlı yöntemler kullanma (D. Yu ve Deng, 2012).

KK-AÖM sınıflandırıcısı, sınıf kısıtlamalı fark vektörleri ve sınıf kısıtlamalı toplam vektörlerinin yapılarını kullanarak girdi katmanından gizli katmana ağırlıkları belirler. Bu algoritmada normalizasyon için CS-ELM kısıt fark vektörleri ile CD-ELM sınıflandırıcı mantığı ile kısıt toplam vektörleri yapılmaktadır. Giriş katmanından gizli katmana kadar olan ağırlıklarda, (W. Zhu vd., 2015) normalize edilmiş toplam örnek vektörleri kullanılır. Bu strateji ile giriş ağırlık parametreleri atanan AÖM'nin klasik AÖM'den daha başarılı sonuçlar verdiği gösterilmiştir. Bu motivasyonla yukarıda belirtilen üç farklı yaklaşım yerine bu atama stratejisi Meta-AÖM'ye uyarlanarak KK-Meta-AÖM dediğimiz yeni bir AÖM yapısı oluşturulmuştur. KK-Meta-AÖM, giriş katmanından gizli katmana bağlantı ağırlıkları atamak için Algoritma 5.4'teki KK-AÖM yapısındaki model parametrelerinin belirleme süreci Meta-AÖM algoritmasına dahil ederek oluşturulmuştur.

Girdi: $\mathcal{N} = \{(\mathrm{x}_i, t_i) \mid \mathrm{x}_i \in \mathbb{R}^n, t_i \in \mathbb{R}^q, i = 1, \ldots, N\}$ // Eğitim kümesi

$\boldsymbol{L}$ // gizli düğüm sayısı

Çıktı: KK-Meta-AÖM'nin model parametreleri, yani, $\boldsymbol{W}_{(n\times L)}$ (ağırlık matrisi) ve $\boldsymbol{b}_{(1\times L)}$ (bias vektörü)

1 *Kısıtlı toplam vektörlerin sayısı* $\lfloor \boldsymbol{L/2} \rfloor$ *'den az olduğu sürece.*

| Aynu sınıftan $\boldsymbol{x}'_c$ ve $\boldsymbol{x}''_c$ eğitim örneklerini rastgele seç ve $\boldsymbol{x}'_c + \boldsymbol{x}''_c$ *toplam vektörünü oluştur;*

| Toplam vektörü $\boldsymbol{w} = \frac{X_c' + X_c''}{\|X_c' + X_c''\|_{L_2}^2}$ ile normalleştirin ve [0, 1] arasındaki değerlerle düzgün bir dağılımdan karşılık gelen bias b'yi rastgele oluştur.

| Ağırlık matrisini oluşturmak için w ve bias b vektörünü kullanın $\boldsymbol{W}_{n\times(\lceil L/2\rceil)}$ ve bias vektor $\boldsymbol{b}_{1\times(\lceil L/2\rceil)}$

2 *Seçilen fark vektörlerinin sayısı* $\boldsymbol{L} - \lceil \boldsymbol{L/2} \rceil$ *'den az olduğu sürece*

| Sırasıyla herhangi iki farklı sınıftan $\boldsymbol{x_{c1}}$ ve $\boldsymbol{x_{c2}}$ eğitim örneklerini rastgele seçin ve $\boldsymbol{x_{c2}} - \boldsymbol{x_{c1}}$ fark vektörünü oluşturun;

| Fark vektörünü normalize etmek için $\boldsymbol{w} = \frac{2(x_{c2} - x_{c1})}{\|x_{c2} - x_{c1}\|_{L_2}^2}$ kullanın ve ilişkili bias $\boldsymbol{b} = \frac{(x_{c1} + x_{c2})^T (x_{c1} - x_{c2})}{\|x_{c2} - x_{c1}\|_{L_2}^2}$'yi belirleyin.

| Ağırlık matrisini oluşturmak için $\boldsymbol{w}$ ve bias $\boldsymbol{b}$ vektörünü kullanın, ağırlık matrisi $\boldsymbol{W}_{n\times(L-\lceil L/2\rceil)}$ ve bias vektörü $\boldsymbol{b}_{1\times(L-\lceil L/2\rceil)}$.

3 Gizli katman düğüm ağırlıklarını oluşturmak için yukarıdakilerini birleştirin $\boldsymbol{W}_{n\times(\lceil L/2\rceil)}$ *ve* $\boldsymbol{W}_{n\times(L-\lceil L/2\rceil)}$, ve gizli katman düğüm bias'larını oluşturmak için $\boldsymbol{b}_{1\times(\lceil L/2\rceil)}$ *ve* $\boldsymbol{b}_{1\times(L-\lceil L/2\rceil)}$ 'leri birleştir.

Algoritma 5.4. KK-Meta-AÖM için model parametrelerinin belirlenmesi

6. SONUÇLAR VE DEĞERLENDİRME

Bu çalışma, düşük maliyetli donanım ve açık kaynaklı yazılımların kullanıldığı bir IoT cihaz tanımlama sistemi önermektedir. Bu sistem, IoT alanındaki fiziksel katmanda güvenlik amacıyla RF parmak izi çalışmalarının yaygınlaşmasına katkı sağlayacaktır. Yani, IoT cihazlarının tanımlanması ve güvenli bir şekilde sınıflandırılması için sinyal yakalama süreçlerini gerçekleştiren bu sistemin, düşük maliyetli donanım ve açık kaynaklı yazılımların kullanılabilirliğini artırması hedeflenmektedir. Bu da IoT alanındaki RF parmak izi çalışmalarının yaygınlaşmasını kolaylaştırarak, güvenlik konusunda önemli bir adım olacaktır. Ayrıca, IoT cihazlarının Wi-Fi iletişimi sırasında kaydedilen orijinal RF parmak izi veri kümesi literatüre sunulmuştur. Bu veri kümesi, IoT cihazlarının iletişim sinyallerinin benzersiz özelliklerini içermekte ve cihazların tanımlanması ve sınıflandırılması için değerli bir kaynak oluşturmaktadır. Bu veri kümesi, IoT cihazlarının RF parmak izlerinin analiz edilmesi ve tanınması için kullanılabilecek potansiyel bilgileri sağlamaktadır. Bu da IoT cihazlarının güvenlik ve tanımlama süreçlerine yönelik daha etkili ve kesin sonuçlar elde etmek için önemli bir adım olarak değerlendirilmektedir. Bu çalışmada, RF parmak izi tanımlamada ilk defa AÖM tabanlı sınıflandırıcılar kullanılmıştır. Özellikle, genelleme yeteneği ile ön plana çıkan Meta-AÖM yapısı bu çalışmada tercih edilmiştir. Bu yapı genellikle regresyon problemlerinde kullanılmaktadır, ancak bu çalışmada sınıflandırma süreçlerine uyarlama yapılmıştır. Bu şekilde, RF parmak izi tanımlama sürecinde AÖM tabanlı sınıflandırıcıların kullanılması, daha doğru ve etkili sonuçların elde edilmesini sağlamaktadır. Meta-AÖM yapısının genelleme yeteneği, IoT cihazlarının tanımlanması ve sınıflandırılması için önemli bir avantaj sağlamaktadır. Ayrıca, RF ve diğer alanlarda literatüre yenilikler getiren ÇK-Meta-AÖM ve KK-Meta-AÖM gibi iki geliştirilmiş algoritma da bulunmaktadır. Bu algoritmalar, RF parmak izi tanımlama sürecinde kullanılarak daha doğru ve etkili sonuçlar elde etmeyi sağlamaktadır. Bu yeni algoritmalar, IoT cihazlarının RF parmak izlerinin tanınması ve sınıflandırılmasında önemli bir ilerleme sağlamaktadır. Bu sayede, daha hassas ve güvenilir bir IoT cihaz tanımlama süreci elde edilebilmektedir. ÇK-Meta-AÖM ve KK-Meta-AÖM gibi geliştirilen algoritmalar, RF ve benzeri alanlarda çalışmalar yürüten araştırmacılar için değerli bir kaynak teşkil etmektedir.

AÖM tabanlı algoritmaları karşılaştıran çalışmamızda Meta-AÖM'nin RF parmak izi alanında uygulanabilirliği ve başarımı görülmektedir (Parmaksız ve Karakuzu, 2022b). K-AÖM'ler (Constrained/Kısıtlı Aşırı Öğrenme Makinaları), temel AÖM'ye göre gelişmiş

doğruluk başarımı sağladığı bildirilmiştir (W. Zhu vd., 2015). Bölüm 5.1.2'de anlattığımız KK-AÖM'nin bu ilk parametre atama süreci Meta-AÖM'ye entegre edilerek yeni bir KK-Meta-AÖM yapısı geliştirilmiştir. Meta-AÖM'nin performansını iyileştirmek için, Bölüm 5.1.3'te verilen ÇK-AÖM mimarisi Meta-AÖM'ye entegre edilerek yeni bir ÇK-Meta-AÖM algoritması geliştirilmiştir. Algoritmalarda M değeri grup sayısını, N ise her gruptaki nöron sayısını temsil eder. Algoritmaların her biri sınıflayıcı olarak 100 kez çalıştırılmış ve elde edilen sonuçlar kaydedilmiştir. Sınıflandırma algoritmalarının her birinde N hücre sayısı {10, 30, 50, 120} kümesindeki değerlerle, ÇK-Meta-AÖM algoritmasında M grup sayısı da boyutsal ve yazılımsal kısıtlamalar dikkate alınarak {30, 58, 145, 174, 261, 522} kümesindeki değerlerle, Meta-AÖM ve KK-Meta-AÖM algoritmalarında ise M {5, 10, 30, 50, 75, 100} kümesindeki değerlerle ayrı ayrı çalıştırılmıştır. ÇK-Meta-AÖM yapısında her bir temel AÖM'deki katman sayısı 3'tür.

6.1. Sonuçlar

Tablo 6.1, 6.2 ve 6.3'te, sınıflandırma topluluk AÖM algoritmalarının M ve N değerlerine bağlı olarak, eğitim ve test aşamalarındaki başarım ve algoritma işletme sürelerinin ortalama, en iyi, en kötü ve standart sapma değerleri sunulmaktadır. Şekil 6.1'de Meta-AÖM algoritmasının eğitim ve testteki sınıflandırma doğruluk yüzdeleri verilmektedir. Şekil 6.2'de aynı algoritmanın sınıflandırmada harcadığı süre saniye cinsinden verilmiştir. Şekil 6.3'te KK-Meta-AÖM algoritmasının eğitim ve test veri kümesi için sınıflandırma doğruluk yüzdeleri verilmektedir. Şekil 6.4'de aynı algoritmanın sınıflandırmada harcadığı süre saniye cinsinden verilmiştir. Bu tablolardan özet grafikler çizilerek ÇK-Meta-AÖM algoritmasının eğitim ve test veri kümesindeki sınıflandırma doğruluk yüzdeleri Şekil 6.5'de verilmiştir. Şekil 6.6'da aynı algoritmanın sınıflandırmada geçirdiği süre saniye cinsinden verilmiştir. . Meta-AÖM, KK-Meta-AÖM ve ÇK-Meta-AÖM algoritmalarının karışıklık matrisleri Şekil 6.7'de verilmiştir.

Tablo 6.1. Meta-AÖM sınıflandırıcının deneysel sonuçları

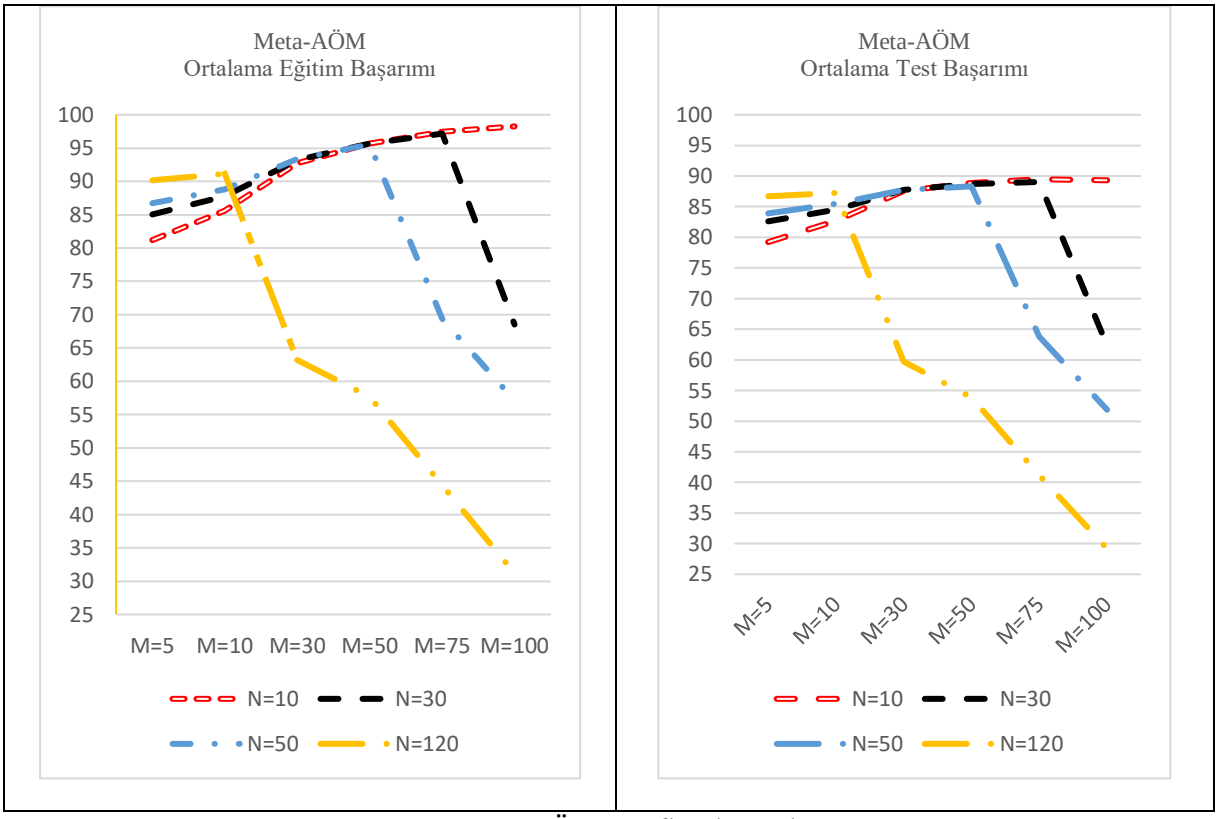
M		N=10				N=30				N=50				N=120			
		Ort	En iyisi	En kötüsü	Std. Sapma	Ort	En iyisi	En kötüsü	Std. Sapma	Ort	En iyisi	En kötüsü	Std. Sapma	Ort	En iyisi	En kötüsü	Std. Sapma
5 Eğitim	Doğr.	0.81192	0.83755	0.77701	0.011278	0.85011	0.87356	0.82682	0.008483	0.86722	0.88352	0.84904	0.006432	0.90204	0.91149	0.88927	0.004353
	Süre	0.51301	0.45547	0.57734	0.034437	0.5341	0.4648	0.59918	0.033975	0.53837	0.46879	0.61605	0.037853	0.61271	0.53327	0.67513	0.035058
5 Test	Doğr.	0.79228	0.83021	0.75871	0.012565	0.82577	0.85255	0.79982	0.010911	0.83921	0.86238	0.81591	0.008381	0.86696	0.88293	0.84987	0.006068
	Süre	0.00430	0.003302	0.006142	0.0005832	0.005694	0.004258	0.007216	0.00070	0.0059333	0.004657	0.00742	0.000631	0.01885	0.01658	0.02217	0.001158
10 Eğitim	Doğr.	0.85604	0.87701	0.83295	0.0093478	0.87739	0.89387	0.86169	0.006189	0.88811	0.90077	0.87433	0.005692	0.91141	0.92222	0.9023	0.003531
	Süre	0.55658	0.51206	0.6056	0.019235	0.56215	0.52422	0.61762	0.020352	0.6023	0.55592	0.64315	0.021224	0.7306	0.65187	0.79591	0.034452
10 Test	Doğr.	0.82693	0.85612	0.80518	0.010698	0.84537	0.86327	0.81144	0.008994	0.85472	0.87131	0.83467	0.006645	0.87247	0.88382	0.8588	0.005914
	Süre	0.00888	0.006327	0.012647	0.0011357	0.010709	0.008413	0.014199	0.00117	0.011694	0.009320	0.01490	0.001262	0.03774	0.03344	0.04619	0.002830
30 Eğitim	Doğr.	0.92704	0.9364	0.91456	0.0047042	0.93236	0.94215	0.92299	0.003851	0.93344	0.94215	0.92529	0.003302	0.6317	0.93027	0.02490	0.3763
	Süre	0.63454	0.57102	0.69384	0.027287	0.69199	0.63573	0.74528	0.024188	0.76168	0.66191	0.83782	0.036793	1.1279	1.0201	1.2855	0.055287
30 Test	Doğr.	0.87556	0.88919	0.85791	0.0069726	0.87714	0.89723	0.86238	0.005965	0.87783	0.89455	0.86416	0.006086	0.59714	0.88204	0.02591	0.34973
	Süre	0.035931	0.027681	0.043078	0.0029872	0.041072	0.033098	0.04744	0.002741	0.046755	0.037508	0.10096	0.006805	0.12314	0.10648	0.18001	0.015376
50 Eğitim	Doğr.	0.95676	0.96284	0.94751	0.0031676	0.95687	0.9636	0.95134	0.002548	0.95556	0.96092	0.94828	0.002441	0.57651	0.9567	0.03295	0.39868
	Süre	0.73901	0.66496	0.83063	0.027583	0.82663	0.76687	0.9091	0.03175	0.91111	0.81035	1.0259	0.034545	1.5258	1.4269	1.6645	0.056175
50 Test	Doğr.	0.8891	0.90706	0.87489	0.0063984	0.88679	0.9008	0.86416	0.006532	0.88317	0.89723	0.8731	0.004896	0.53851	0.90349	0.03127	0.36258
	Süre	0.07238	0.059369	0.089095	0.0059514	0.085031	0.072876	0.099764	0.005243	0.082543	0.072867	0.09688	0.003535	0.21517	0.19169	0.25927	0.011195
75 Eğitim	Doğr.	0.97423	0.97778	0.96973	0.0016377	0.97168	0.97548	0.96667	0.001884	0.69315	0.97356	0.05134	0.38566	0.44346	0.97356	0.01571	0.38925
	Süre	0.87168	0.8119	0.95287	0.027669	1.0155	0.94928	1.1168	0.038734	1.1305	1.0151	1.2996	0.068866	2.1441	1.9693	2.3711	0.081984
75 Test	Doğr.	0.89477	0.90974	0.88204	0.005548	0.89039	0.91332	0.87578	0.006514	0.6378	0.89812	0.07775	0.34616	0.41137	0.89276	0.02413	0.34823
	Süre	0.1294	0.11027	0.18978	0.010615	0.14485	0.12431	0.20363	0.013587	0.14326	0.12501	0.17399	0.01155	0.34701	0.30609	0.42472	0.022028
100 Eğitim	Doğr.	0.98261	0.98582	0.97778	0.0015793	0.68521	0.98429	0.072414	0.39595	0.57101	0.98161	0.0084291	0.42645	0.31186	0.98084	0.008046	0.33519
	Süre	1.1301	1.0515	1.2352	0.037293	1.314	1.1974	1.4614	0.060256	1.6256	1.4844	1.8038	0.052591	2.7506	2.5114	2.9689	0.092933
100 Test	Doğr.	0.89269	0.90617	0.87757	0.0062429	0.6234	0.89991	0.076854	0.35069	0.51852	0.89455	0.018767	0.37709	0.29189	0.88651	0.020554	0.29384
	Süre	0.21455	0.17738	0.33327	0.02229	0.23302	0.19575	0.26613	0.0154	0.24093	0.20111	0.32522	0.019519	0.50121	0.44748	0.55577	0.026835

Tablo 6.2. KK-Meta-AÖM sınıflandırıcının deneysel sonuçları

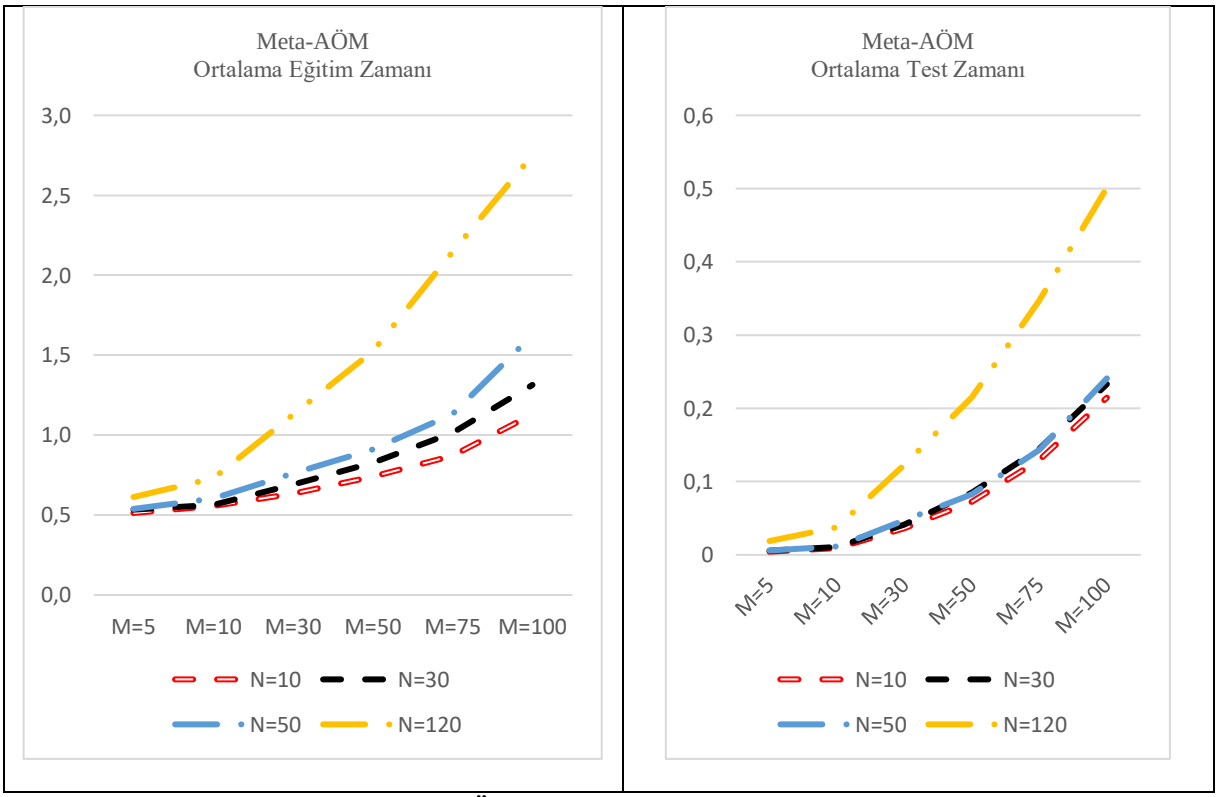
M		N=10				N=30				N=50				N=120			
		Ort	En iyisi	En kötüsü	Std. Sapma	Ort	En iyisi	En kötüsü	Std. Sapma	Ort	En iyisi	En kötüsü	Std. Sapma	Ort	En iyisi	En kötüsü	Std. Sapma
5 Eğitim	Doğr.	0.89759	0.91303	0.82375	0.01247	0.91115	0.91724	0.90153	0.00292	0.91686	0.92337	0.90996	0.00260	0.92948	0.93563	0.92414	0.00267
	Süre	0.52851	0.46933	0.59617	0.03477	0.52879	0.46639	0.59885	0.03396	0.54235	0.48324	0.61002	0.03310	0.5893	0.52039	0.65144	0.03176
5 Test	Doğr.	0.87271	0.89097	0.80429	0.013119	0.88443	0.89366	0.87131	0.004324	0.88886	0.89723	0.87846	0.003709	0.89796	0.90885	0.8874	0.00371
	Süre	0.004637	0.00323	0.007771	0.000765	0.0057943	0.0043802	0.0072759	0.000745	0.0061	0.0046779	0.008151	0.000805	0.018762	0.016433	0.022086	0.00133
10 Eğitim	Doğr.	0.9168	0.92605	0.88966	0.004212	0.92023	0.92644	0.91379	0.002597	0.92365	0.93103	0.91686	0.002650	0.9314	0.93716	0.92605	0.00245
	Süre	0.54345	0.48005	0.60526	0.034058	0.55034	0.48877	0.61085	0.033672	0.57375	0.51428	0.64677	0.032065	0.67121	0.59633	0.72647	0.03051
10 Test	Doğr.	0.88722	0.89723	0.86327	0.005486	0.89001	0.89902	0.88025	0.004225	0.89315	0.9017	0.88651	0.003591	0.89962	0.90795	0.88919	0.00371
	Süre	0.00887	0.00649	0.01104	0.001063	0.011127	0.0086653	0.014633	0.001201	0.011319	0.0092192	0.014354	0.0014099	0.039238	0.033798	0.049215	0.00404
30 Eğitim	Doğr.	0.95261	0.959	0.94751	0.0022391	0.95615	0.96092	0.95057	0.002157	0.95606	0.96284	0.94904	0.002439	0.56641	0.959	0.066284	0.39617
	Süre	0.65223	0.57335	0.73842	0.035068	0.69056	0.6339	0.74731	0.026333	0.76777	0.69563	0.8263	0.028787	1.0319	0.93517	1.1671	0.04550
30 Test	Doğr.	0.90806	0.92404	0.89723	0.0047258	0.9141	0.92851	0.89991	0.005033	0.91124	0.92404	0.9017	0.0045813	0.54206	0.91689	0.075067	0.37492
	Süre	0.035028	0.027819	0.042452	0.0036958	0.042642	0.034051	0.052049	0.003786	0.044623	0.035276	0.059905	0.0043546	0.12546	0.1069	0.15618	0.01152
50 Eğitim	Doğr.	0.97051	0.97356	0.96705	0.0012017	0.97091	0.97471	0.96743	0.001343	0.97041	0.97318	0.96705	0.001268	0.5952	0.97395	0.075479	0.40444
	Süre	0.77753	0.71169	0.84349	0.026459	0.83641	0.76019	0.89209	0.031047	0.95123	0.88098	1.0075	0.026845	1.3699	1.2762	1.4921	0.04372
50 Test	Doğr.	0.92239	0.93119	0.91063	0.0043867	0.92584	0.93476	0.91689	0.0038201	0.92426	0.93298	0.91153	0.003734	0.56811	0.9294	0.069705	0.38119
	Süre	0.075622	0.061877	0.10066	0.0069646	0.086745	0.070682	0.10567	0.0075832	0.090358	0.077224	0.10922	0.007339	0.23308	0.2085	0.29215	0.01522
75 Eğitm	Doğr.	0.98006	0.98276	0.97739	0.0011192	0.97321	0.98314	0.22146	0.075943	0.5997	0.98276	0.078161	0.3987	0.55344	0.98429	0.072414	0.41882
	Süre	0.97089	0.88595	1.0457	0.033728	1.0336	0.9546	1.1633	0.038581	1.2245	1.1001	1.3397	0.041573	1.8514	1.7035	2.0153	0.06002
75 Test	Doğr.	0.92575	0.93566	0.91778	0.0036108	0.91888	0.93387	0.23414	0.069252	0.56916	0.93566	0.079535	0.37261	0.5236	0.93119	0.075961	0.38936
	Süre	0.13682	0.11304	0.2709	0.018636	0.15041	0.12531	0.20229	0.014335	0.1555	0.12985	0.18622	0.013339	0.38292	0.34469	0.45226	0.02249
100 Eğitim	Doğr.	0.98491	0.98659	0.98199	0.000872	0.61153	0.98736	0.086973	0.40095	0.55749	0.98927	0.081992	0.41404	0.36646	0.98774	0.001532	0.36221
	Süre	1.1708	1.0547	1.3066	0.053672	1.2994	1.1997	1.4268	0.053012	1.5519	1.4114	1.6709	0.049785	2.3554	2.1847	2.5215	0.07489
100 Test	Doğr.	0.92421	0.93476	0.9151	0.003735	0.57742	0.93208	0.074173	0.37128	0.52507	0.93029	0.06881	0.38257	0.34795	0.92493	0.00178	0.33334
	Süre	0.20613	0.1758	0.26016	0.0147	0.23154	0.20272	0.30011	0.01799	0.23804	0.19873	0.27588	0.02009	0.52144	0.46473	0.66893	0.03392

Tablo 6.3. ÇK-Meta-AÖM sınıflandırıcının deneysel sonuçları

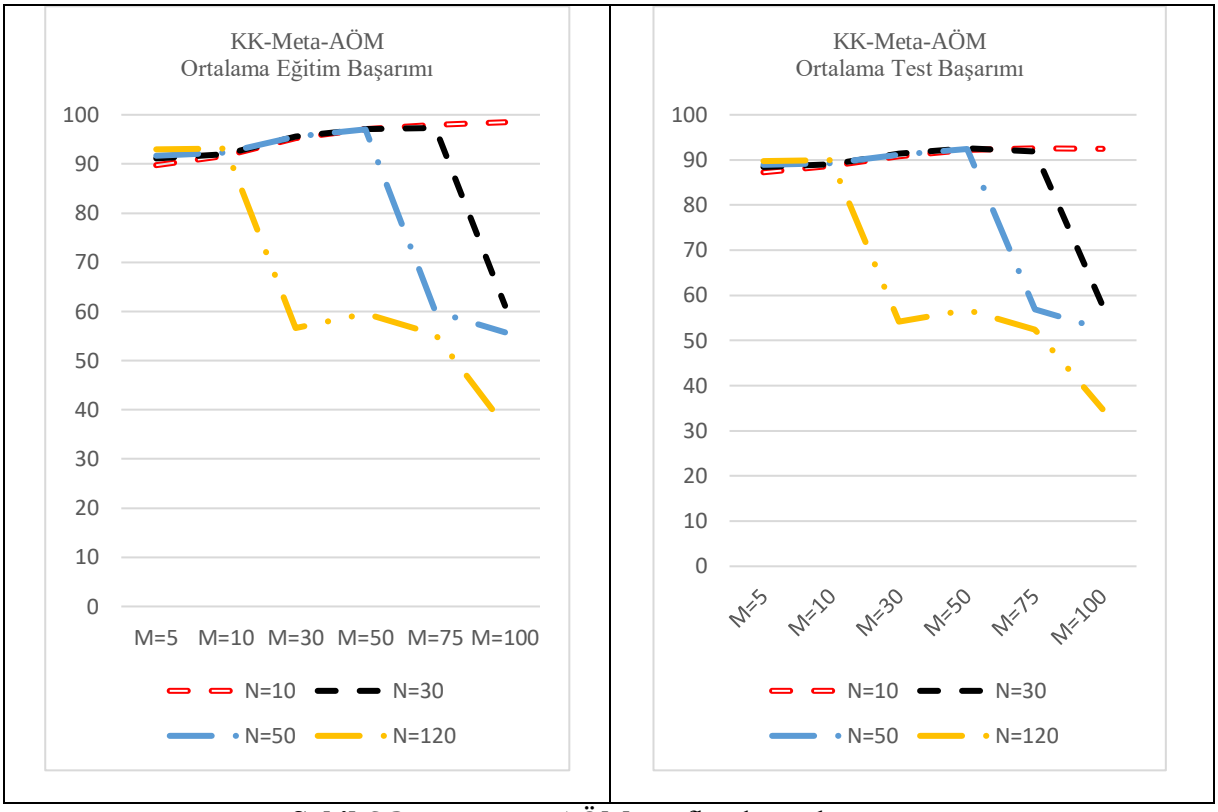
M		N=10				N=30				N=50				N=120			
		Ort	En iyisi	En kötüsü	Std. Sapma	Ort	En iyisi	En kötüsü	Std. Sapma	Ort	En iyisi	En kötüsü	Std. Sapma	Ort	En iyisi	En kötüsü	Std. Sapma
30 Eğitim	Doğr.	0.7450	0.8337	0.6084	0.0511	0.8070	0.8690	0.7287	0.0284	0.8376	0.8820	0.7755	0.0206	0.9000	0.9157	0.8736	0.0074
	Süre	0.5027	0.4258	0.6000	0.0420	0.6152	0.5304	0.7035	0.0463	0.7279	0.6168	0.8546	0.0561	1.4340	1.2349	1.6256	0.0885
30 Test	Doğr.	0.7199	0.8123	0.5719	0.0496	0.7651	0.8400	0.6836	0.0303	0.7905	0.8409	0.7310	0.0225	0.8482	0.8811	0.8204	0.0104
	Süre	0.1120	0.1002	0.1329	0.0072	0.1228	0.1072	0.1573	0.0113	0.1281	0.1118	0.1610	0.0126	0.2527	0.2153	0.3109	0.0241
58 Eğitim	Doğr.	0.8371	0.8969	0.7713	0.0281	0.8562	0.9123	0.8011	0.0222	0.9141	0.9318	0.8912	0.0076	0.9456	0.9521	0.9330	0.0034
	Süre	1.4760	1.2976	1.6386	0.0565	1.2479	1.0351	1.4749	0.0900	1.5109	1.3028	1.7791	0.1166	2.8756	2.4934	3.3114	0.1571
58 Test	Doğr.	0.7872	0.8490	0.7069	0.0271	0.7962	0.8472	0.7364	0.0236	0.8399	0.8713	0.8123	0.0121	0.8756	0.8954	0.8561	0.0070
	Süre	0.3990	0.3656	0.4459	0.0180	0.2592	0.2291	0.3220	0.0205	0.2631	0.2346	0.3554	0.0271	0.5265	0.4559	0.6709	0.0489
100 Eğitim	Doğr.	0.8532	0.8985	0.7575	0.0259	0.9240	0.9456	0.9027	0.0084	0.9522	0.9632	0.9425	0.0044	0.9676	0.9739	0.9605	0.0024
	Süre	1.8410	1.6234	2.0507	0.0739	2.2897	2.0388	2.5693	0.1196	2.7286	2.4885	2.9355	0.1017	4.8674	4.6033	5.4305	0.1393
100 Test	Doğr.	0.7987	0.8400	0.7203	0.0246	0.8336	0.8588	0.8105	0.0105	0.8605	0.8811	0.8382	0.0088	0.8836	0.8963	0.8695	0.0061
	Süre	0.4632	0.4016	0.5270	0.0275	0.4892	0.4321	0.5485	0.0274	0.5095	0.4602	0.5702	0.0268	0.9283	0.8535	1.0547	0.0383
174 Eğitim	Doğr.	0.8882	0.9195	0.8414	0.0166	0.9608	0.9690	0.9494	0.0036	0.9734	0.9789	0.9667	0.0024	0.9866	0.9904	0.9831	0.0016
	Süre	3.0222	2.8045	3.2852	0.0862	4.4969	3.9988	4.8455	0.1577	5.2531	4.8274	5.8548	0.2081	9.2670	8.8108	10.0778	0.2260
174 Test	Doğr.	0.8137	0.8481	0.7748	0.0177	0.8403	0.8570	0.8168	0.0078	0.8547	0.8758	0.8311	0.0072	0.8839	0.9008	0.8722	0.0054
	Süre	0.9498	0.8818	1.0274	0.0279	1.0453	0.9403	1.1508	0.0395	1.0568	0.9478	1.1466	0.0436	1.8238	1.6940	2.0439	0.0691
261 Eğitim	Doğr.	0.9281	0.9502	0.8897	0.0096	0.9757	0.9812	0.9705	0.0023	0.9852	0.9893	0.9797	0.0018	0.9960	0.9981	0.9935	0.0010
	Süre	5.4710	5.2206	5.7243	0.1152	7.8104	7.2198	8.3543	0.2549	9.0443	8.4505	9.6246	0.2570	15.3984	14.1129	16.4138	0.3910
261 Test	Doğr.	0.8306	0.8606	0.7962	0.0109	0.8256	0.8472	0.7945	0.0107	0.8326	0.8579	0.8097	0.0099	0.8759	0.8901	0.8597	0.0056
	Süre	1.6894	1.5886	1.8027	0.0439	1.8489	1.7444	1.9410	0.0413	1.9053	1.7864	2.0239	0.0504	3.1321	2.9298	3.4910	0.1042
522 Eğitim	Doğr.	0.9665	0.9743	0.9605	0.0031	0.9927	0.9969	0.9897	0.0016	0.9985	0.9996	0.9962	0.0008	0.9998	1.0000	0.9992	0.0002
	Süre	14.8355	14.2157	15.3808	0.2413	16.9604	14.5235	17.6887	0.5133	19.6722	18.9150	20.4112	0.2914	34.9506	32.7180	36.1272	0.6839
522 Test	Doğr.	0.8273	0.8517	0.7980	0.0111	0.7041	0.7721	0.6452	0.0265	0.7796	0.8186	0.7364	0.0190	0.8558	0.8794	0.8374	0.0074
	Süre	4.9288	4.7027	5.1985	0.1137	5.3066	4.6041	5.5856	0.1735	5.4977	5.2299	5.7344	0.1033	7.6074	7.1646	8.1085	0.1810



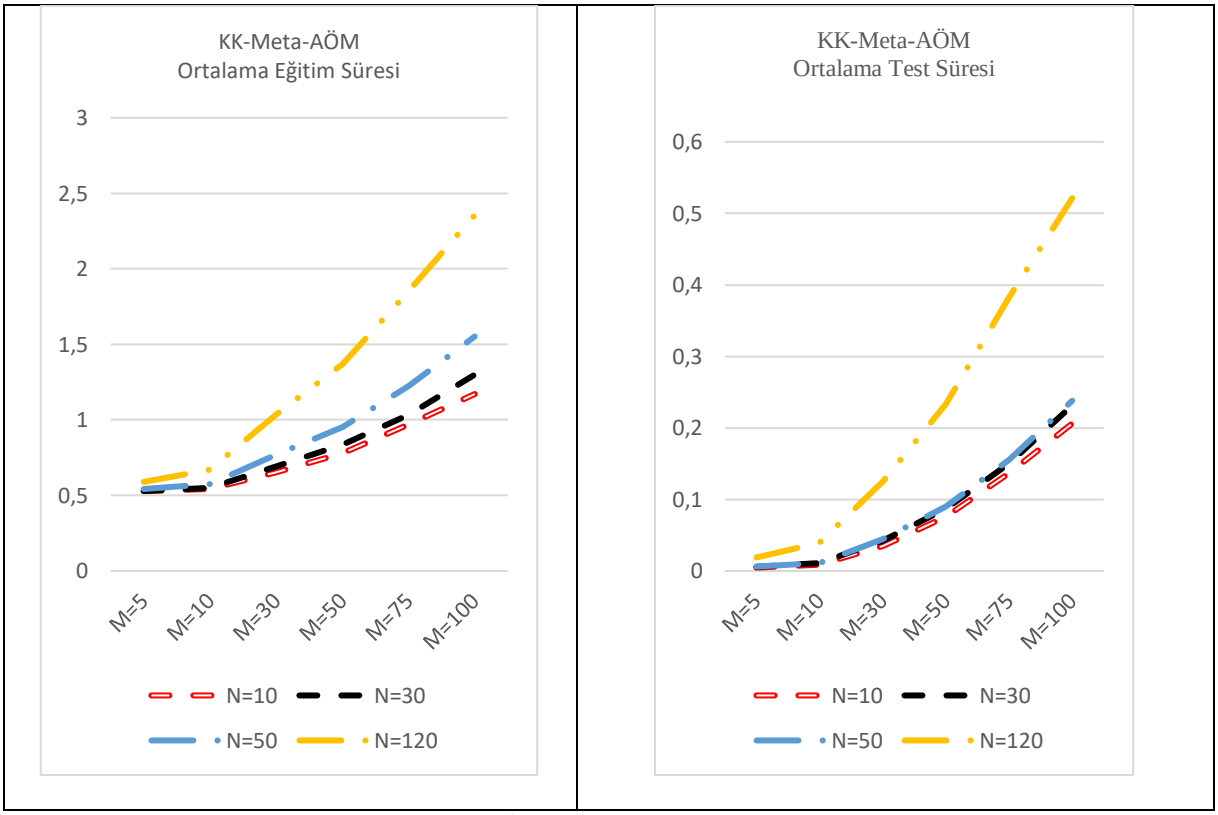
Şekil 6.1. Meta-AÖM sınıflandırma başarımı



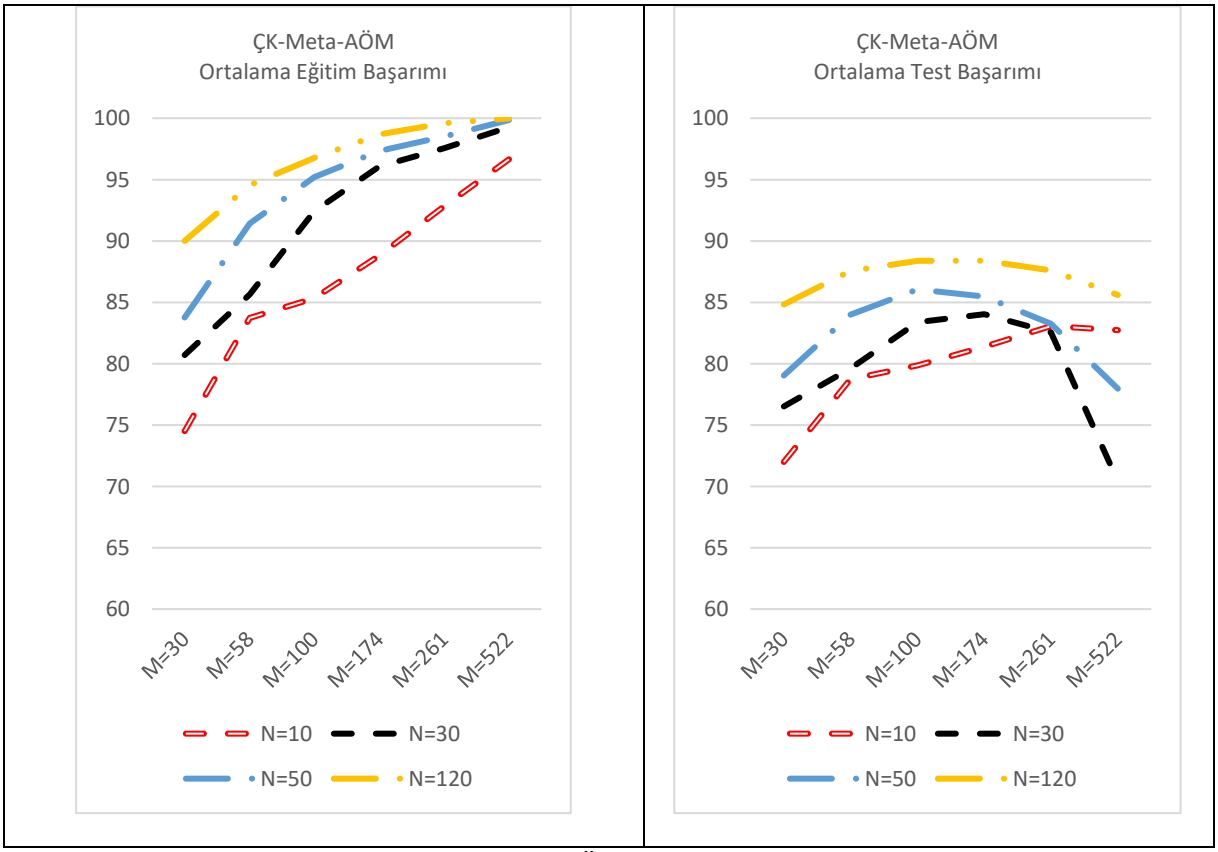
Şekil 6.2. Meta-AÖM sınıflandırıcı eğitim ve test süreleri



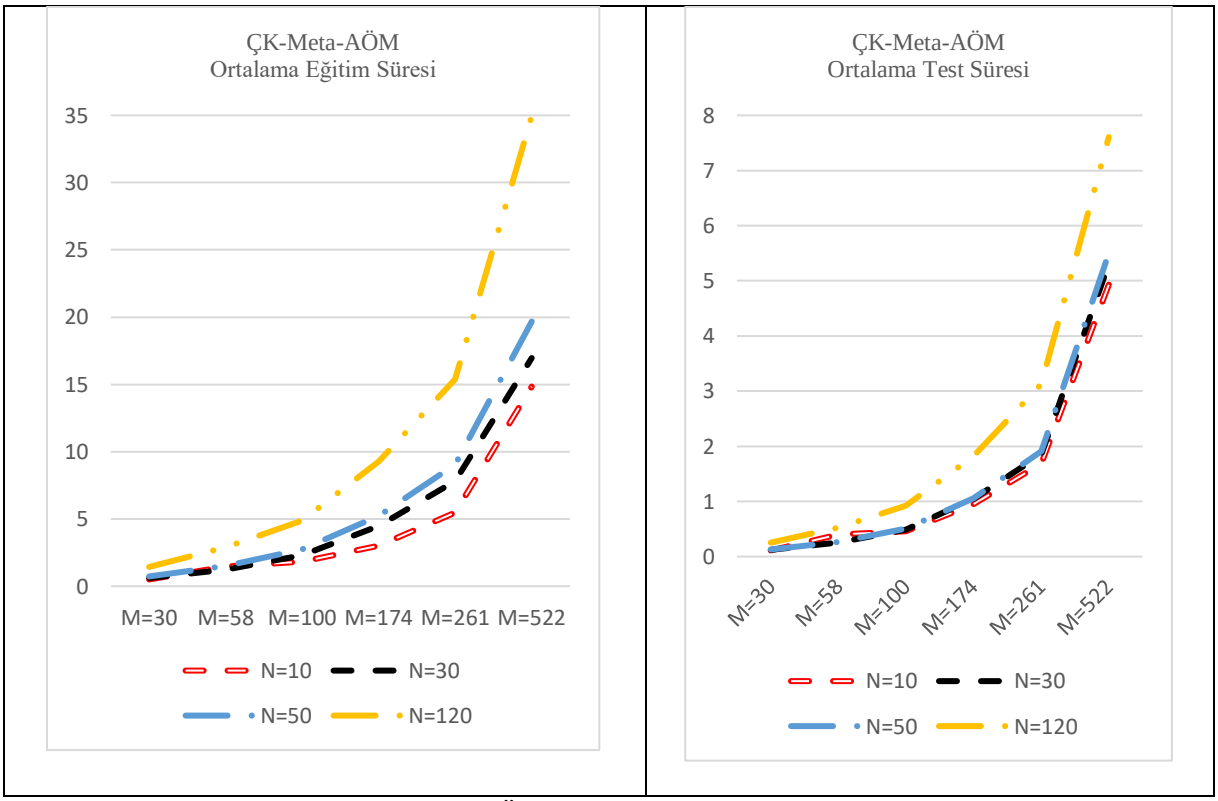
Şekil 6.3. KK-Meta-AÖM sınıflandırma başarımı



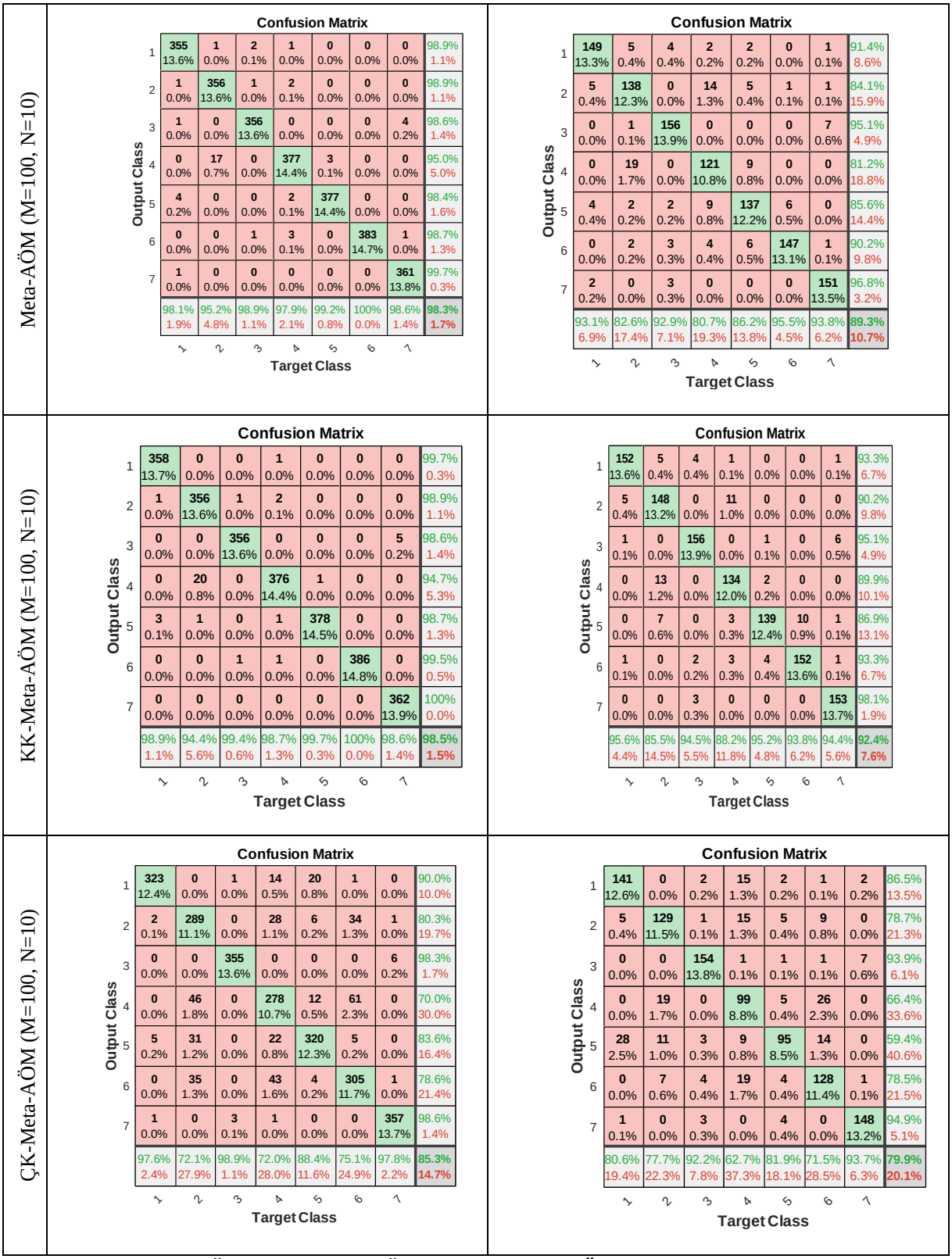
Şekil 6.4. KK-Meta-AÖM sınıflandırıcı eğitim ve test süreleri



Şekil 6.5. ÇK-Meta-AÖM sınıflandırma başarımı



Şekil 6.6. ÇK-Meta-AÖM sınıflandırıcı eğitim ve test süreleri



Şekil 6.7. Meta-AÖM, KK-Meta-AÖM ve ÇK-Meta-AÖM sınıflandırıcı algoritmalarının karışıklık matrisleri (sol: eğitim verileri, sağ: test verileri)

6.2. Değerlendirme

Tezde, yeni bir IoT cihaz tanımlama sistemi önerilmiştir. Sinyal yakalama süreçlerinde düşük maliyetli donanım ve yazılımlara sahip yapısı, bu alandaki çalışmaların yaygınlaşmasını kolaylaştıracaktır. Detayları Tablo 4.2'de verilen 7 IoT cihazın Wi-Fi iletişimi sırasında elde edilen orijinal bir RF parmak izi veri kümesi literatüre kazandırılmıştır. İlk kez bu çalışmada AÖM tabanlı sınıflandırıcılar RF parmak izi tanımada kullanılmaktadır. AÖM yapıları arasında genelleme yeteneği ile ön plana çıkan Meta-AÖM yapısı bu çalışmada özellikle tercih edilmiştir. Meta-AÖM'nin genellikle regresyon problemlerinde kullanıldığı görülmektedir. Sınıflandırma süreçlerine uyarladığımız Meta-AÖM algoritmasının ve geliştirdiğimiz diğer iki algoritmanın (ÇK-Meta-AÖM ve KK-Meta-AÖM) kullanımı RF ve diğer alanlarda literatüre yenilikler sunacaktır. Tezimizde geliştirilen ve kullanılan AÖM yapıları topluluğunun başarım açısından, bu çalışmada kullanılan RF parmak izi veri kümesi çerçevesinde aşağıdaki hususlar belirlenmiştir:

• Şekil 6.1'de Meta-AÖM algoritmasının eğitim aşaması için N=10 için %98,26 maksimum doğruluğa ulaştığı görülmektedir. Test aşamasında maksimum %89.99 doğruluğa ulaşabildiği gözlemlenmiştir. Algoritmada M grup sayısı arttıkça başarımda artış gözlemlenirken, gruplardaki hücre sayısındaki artış başarımı keskin bir şekilde düşürmüştür. Bu özellikle N=120 için belirgindir. Şekil 6.3'te KK-Meta-AÖM algoritmasının eğitim aşamasında N=10 için maksimum %98,49 doğruluğa ulaşabildiği görülmektedir. Test aşamasında maksimum %92,57 doğruluğa ulaşabildiği gözlemlenmiştir.

• Şekil 6.1 ve Şekil 6.3'te görüldüğü gibi Meta-AÖM ve KK-Meta-AÖM ağlarının başarımlarının hem eğitim hem de test aşamalarında benzer bir genel görünüme sahip olduğu görülmektedir. KK-Meta-AÖM, bazı durumlarda Meta-AÖM'ye kıyasla eğitim kümesi için %6'ya kadar başarım artışı ve test kümesi için %4'e kadar başarım artışı sağladığı gözlemlenmiştir. Bu, geliştirilmiş KK-Meta-AÖM ağının genelleme yeteneğinin Meta-AÖM ağına kıyasla geliştirildiğini gösteren bir kanıttır.

• Şekil 6.2 ve 6.4'teki zaman boyutu karşılaştırıldığında, KK-Meta-AÖM ağının hem eğitim hem de test aşamalarında Meta-AÖM ile aynı hızda çalıştığı görülmektedir. Bu da gerçek uygulamalarda hızdan ödün vermeden daha başarımlı bir ağ yapısının elde edildiğini göstermektedir.

• Şekil 6.1 ve 6.5 karşılaştırıldığında görülebileceği gibi, ÇK-Meta-AÖM ağı, her iki fazda da Meta-AÖM'ye göre tüm gruplar ve hücre sayıları için başarımda herhangi bir kesinti olmaksızın sağlam bir başarım seyrine sahiptir, ancak doğruluk başarımı açısından bir tık geride kalmaktadır.

• Şekil 6.5'da ÇK-Meta-AÖM algoritmasının eğitim aşamasında M=522, N=120 için maksimum ortalama %99,98 doğruluk oranına ulaşabildiği görülmektedir. Test aşamasında M=174, N=120 için maksimum ortalama doğruluk oranlarının %88,39'a ulaştığı gözlemlendi. Bu sonuç, ÇK-Meta-AÖM'nin en azından bu uygulama için biraz daha ezberleyici bir yapı olduğunu göstermektedir.

• Öte yandan, ÇK-Meta-AÖM ağının zaman boyutunda her iki faz için de oldukça yavaş çalıştığı açıktır. Bu ağ yapısının ancak AÖM grubu sayısı az olan gerçek zamanlı uygulamalarda kullanılabileceği söylenebilir.

Hem AÖM yapılarının RF parmak izi tanımada kullanımının ilk olması hem de yukarıda tanımladığımız KK-Meta-AÖM ile ÇK-Meta-AÖM grup öğrenme mimari ve algoritmalarının geliştirilmesi bu tez çalışmasının özgün ve dikkate değer yanlarındandır. Geliştirilen algoritmaların farklı sınıflandırma problemlerinde kullanılması literaüre yenilik katacağı düşünülmektedir.

6.3. Akademik Katkılar

- Uygun maliyetli donanımlar ve açık kaynak yazılımlar ile RF sinyal yakalama sistemi oluşturuldu.
- Literatürdeki örnek RF kümelerinde kullanılan özniteliklere özellik çıkarma yöntemleri uygulanarak özgün öznitelikler oluşturuldu.
- Literatüre özgün RF veri kümesi kazandırıldı.
- AÖM tabanlı sınıflandırıcıların RF parmak izi tanımlama sistemlerinde ilk kez kullanılmasına öncülük edildi.
- Meta-AÖM ve bu çalışma kapsamında geliştirilen, KK-Meta-AÖM ve ÇK-Meta-AÖM sınıflandırıcı algoritmaların bu alanda başarımları değerlendirildi.

6.4. Yayınlar

- TR dizindeki uluslararası bir dergi olan Sakarya University Journal of Computer and Information Sciences'ta literatürdeki RF parmak izi çalışmalarını özetleyen bir derleme

(review) makale yayınlandı. (Parmaksız, H., & Karakuzu, C., A Review of Recent Developments on Secure Authentication Using RF Fingerprints Techniques, Sakarya University Journal of Computer and Information Sciences (Online) , cilt.5, sa.3, ss.278-303, 2022)

- Ulusal bir dergi olan Rahva Journal of Technical and Social Studies'te RF parmak izi elde edilmesi için gereken süreç ve materyaller ile ilgili bir araştırma makalesi yayınlandı. (Parmaksız, H., & Karakuzu, C., Yazılım Tanımlı Radyoya Dayalı RF Parmak İzi Toplamak için Düşük Maliyetli Bir Çözüm, Rahva Teknik ve Sosyal Araştırmalar Dergisi , cilt.2, sa.2, ss.179-188, 2022)
- Uluslararası bir dergi olan BSEUJERT'te JOA-VK'den (örnek RF ham sinyal) RF parmak izi elde edilerek sonrasında ilgili parmak-izleri için AÖM, Kısıtlı (Constrained) AÖM'ler ve Meta-AÖM algoritmalarının sınıflandırma başarımını gösteren bir makale yayınlandı. (Parmaksız, H., & Karakuzu, C., Performance analysis of Extreme Learning Machine Classifiers on Radio Frequency Fingerprint, BSEU Journal of Engineering Research and Technology , cilt.3, sa.2, ss.1-7, 2022)

KAYNAKÇA

Abbas, S., Nasir, Q., Nouichi, D. vd. (2021). Improving security of the Internet of Things via RF fingerprinting based device identification system. Neural Computing and Applications, 33(21), 14753-14769.

Abirami, M., Hariharan, V., Sruthi, M. vd. (2013). Exploiting GNU radio and USRP: an economical test bed for real time communication systems. *2013 fourth international conference on computing, communications and networking technologies (ICCCNT)*, s. 1-6.

Aghnaiya, A., Dalveren, Y., & Kara, A. (2020). On the performance of variational mode decomposition-based radio frequency fingerprinting of Bluetooth devices. *Sensors, 20*(6), 1704.

Akeela, R., & Dezfouli, B. (2018). Software-defined Radios: Architecture, state-of-the-art, and challenges. *Computer Communications, 128*, 106-125.

Akhtyamov, R., Golkar, A., & Hanson, M. (2015). Development and stratospheric flight demonstration of a SDR-enabled Federated System. *Jun-2015.[Online]. Available: https://www. researchgate. net/profile/Rustam_Akhtyamov/publication/282279134_Development_and_stratospheric_flight_demonstration_o f_a_SDR-enabled_Federated_System/links/560a4bdb08ae1396914bb27c. pdf.[Accessed: 14-Jan-2020]*.

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K. vd. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE communications surveys & tutorials, 22*(3), 1646-1685.

Al-Shawabka, A., Restuccia, F., D'Oro, S. vd. (2020). Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting. *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, s. 646-655.

Al-Shawabka, A., Restuccia, F., D'Oro, S. vd. (2020). Massive-Scale I/Q Datasets for WiFi Radio Fingerprinting. *Computer Networks, 182*, 107566.

Alsahlany, A. M., Alfatlawy, Z. H., & Almusawy, A. R. (2018). Experimental Evaluation of Different Penetration Security Levels in Wireless Local Area Network. *J. Commun., 13*(12), 723-729.

Amanullah, M. A., Habeeb, R. A. A., Nasaruddin, F. H. vd. (2020). Deep learning and big data technologies for IoT security. *Computer Communications, 151*, 495-517.

Angeletti, P., Lisi, M., & Tognolatti, P. (2014). Software Defined Radio: A key technology for flexibility and reconfigurability in space applications. *2014 IEEE Metrology for Aerospace (MetroAeroSpace)*, s. 399-403.

Angueira, P., Val, I., Montalban, J. vd. (2022). A survey of physical layer techniques for secure wireless communications in industry. *IEEE communications surveys & tutorials, 24*(2), 810-838.

Bakırcı, A. (2019). *Aşırı öğrenme makineleri ile dinamik sistem modelleme.* Bilecik Şeyh Edebali Üniversitesi, Fen Bilimleri Enstitüsü.

Baldini, G., & Steri, G. (2017). A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components. *IEEE communications surveys & tutorials, 19*(3), 1761-1789.

Barbeau, M., Hall, J., & Kranakis, E. (2006). Detection of rogue devices in bluetooth networks using radio frequency fingerprinting. *proceedings of the 3rd IASTED International Conference on Communications and Computer Networks, CCN*, s. 4-6.

Bassey, J., Adesina, D., Li, X. vd. (2019). Intrusion detection for IoT devices based on RF fingerprinting using deep learning. *2019 Fourth International Conference on Fog and mobile edge computing (FMEC)*, s. 98-104.

Bertoncini, C., Rudd, K., Nousain, B. vd. (2011). Wavelet fingerprinting of radio-frequency identification (RFID) tags. *IEEE Transactions on Industrial Electronics, 59*(12), 4843-4850.

Bloessl, B., Segata, M., Sommer, C. vd. (2013). An IEEE 802.11 a/g/p OFDM Receiver for GNU Radio. *Proceedings of the second workshop on Software radio implementation forum*, s. 9-16.

Brik, V., Banerjee, S., Gruteser, M. vd. (2008). Wireless device identification with radiometric signatures. *Proceedings of the 14th ACM international conference on Mobile computing and networking*, s. 116-127.

Chatterjee, B., Das, D., Maity, S. vd. (2018). RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning. *IEEE Internet of Things Journal, 6*(1), 388-398.

Chen, L., Zhao, C., Zheng, Y. vd. (2021). Radio Frequency Fingerprint Identification Based on Transfer Learning. *2021 IEEE/CIC International Conference on Communications in China (ICCC)*, s. 81-85.

Chen, S., Wen, H., Wu, J. vd. (2019). Radio frequency fingerprint-based intelligent mobile edge computing for internet of things authentication. *Sensors*, *19*(16), 3610.

Chen, Y., Lu, S., Kim, H.-S. vd. (2016). A low power software-defined-radio baseband processor for the Internet of Things. *2016 IEEE international symposium on high performance computer architecture (HPCA)*, s. 40-51.

Cobb, W. E., Garcia, E. W., Temple, M. A. vd. (2010). Physical layer identification of embedded devices using RF-DNA fingerprinting. *2010-Milcom 2010 Military Communications Conference*, s. 2168-2173.

Danev, B., & Capkun, S. (2009). Transient-based identification of wireless sensor nodes. *2009 International Conference on Information Processing in Sensor Networks*, s. 25-36.

Danev, B., Heydt-Benjamin, T. S., & Capkun, S. (2009). Physical-layer Identification of RFID Devices. *USENIX security symposium*, s. 199-214.

Danev, B., Zanetti, D., & Capkun, S. (2012). On physical-layer identification of wireless devices. *ACM Computing Surveys (CSUR)*, *45*(1), 1-29.

Ding, L., Wang, S., Wang, F. vd. (2018). Specific emitter identification via convolutional neural networks. *IEEE Communications Letters*, *22*(12), 2591-2594.

Ezuma, M., Erden, F., Anjinappa, C. K. vd. (2019). Micro-UAV detection and classification from RF fingerprints using machine learning techniques. *2019 IEEE Aerospace Conference*, s. 1-13.

Ezuma, M., Erden, F., Anjinappa, C. K. vd. (2020). Drone remote controller RF signal dataset. *IEEE Dataport*.

Ghosh, A. M., & Grolinger, K. (2019). Deep learning: Edge-cloud data analytics for iot. *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, s. 1-7.

Gravelle, C., & Zhou, R. (2019). SDR Demonstration of Signal Classification in Real-Time Using Deep Learning. *2019 IEEE Globecom Workshops (GC Wkshps)*, s. 1-5.

Gummineni, M., & Polipalli, T. R. (2020). Implementation of reconfigurable transceiver using GNU Radio and HackRF One. *Wireless Personal Communications*, 1-17.

Hall, J., Barbeau, M., & Kranakis, E. (2004). Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. *Communications, internet, and information technology, 1*.

Huang, D., Al-Hourani, A., Sithamparanathan, K. vd. (2021). Deep learning methods for device authentication using rf fingerprinting. *2021 15th International Conference on Signal Processing and Communication Systems (ICSPCS)*, s. 1-7.

Huang, G.-B., & Siew, C.-K. (2004). Extreme learning machine: RBF network case. *ICARCV 2004 8th Control, Automation, Robotics and Vision Conference, 2004.*, s. 1029-1036.

Huang, G.-B., Zhou, H., Ding, X. vd. (2011). Extreme learning machine for regression and multiclass classification. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 42*(2), 513-529.

Huang, G.-B., Zhu, Q.-Y., & Siew, C.-K. (2004). Extreme learning machine: a new learning scheme of feedforward neural networks. *2004 IEEE international joint conference on neural networks (IEEE Cat. No. 04CH37541)*, s. 985-990.

Huang, G.-B., Zhu, Q.-Y., & Siew, C.-K. (2006). Extreme learning machine: theory and applications. *Neurocomputing, 70*(1-3), 489-501.

Huang, L., Gao, M., Zhao, C. vd. (2013). Detection of Wi-Fi transmitter transients using statistical method. *2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2013)*, s. 1-5.

Huang, Y. (2017). Radio frequency fingerprint extraction of radio emitter based on I/Q imbalance. *Procedia computer science, 107*, 472-477.

Ishkaev, I. R., Shevelev, A. E., Ovsyannikova, A. S. vd. (2018). Possibility of peak-to-avegare power ratio reduction by application of optimal signal for transmitter based on SDR HackRF One. *2018 IEEE International Conference on Electrical Engineering and Photonics (EExPolytech)*, s. 141-145.

Jagannath, A., Jagannath, J., & Kumar, P. S. P. V. (2022). A Comprehensive Survey on Radio Frequency (RF) Fingerprinting: Traditional Approaches, Deep Learning, and Open Challenges. *arXiv preprint arXiv:2201.00680*.

Jagannath, J., Saarinen, H. M., & Drozd, A. L. (2015). Framework for automatic signal classification techniques (FACT) for software defined radios. *2015 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, s. 1-7.

Jana, S., & Kasera, S. K. (2008). On fast and accurate detection of unauthorized wireless access points using clock skews. *Proceedings of the 14th ACM international conference on Mobile computing and networking*, s. 104-115.

Jian, T., Rendon, B. C., Ojuba, E. vd. (2020). Deep learning for RF fingerprinting: A massive experimental study. *IEEE Internet of Things Magazine, 3*(1), 50-57.

Jiang, Y., Peng, L., Hu, A. vd. (2019). Physical layer identification of LoRa devices using constellation trace figure. *EURASIP Journal on Wireless Communications and Networking, 2019*, 1-11.

Kale, G. A., & Karakuzu, C. (2022). Multilayer extreme learning machines and their modeling performance on dynamical systems. *Applied Soft Computing, 122*, 108861.

Karakuzu, C. (2020). İki Yeni Çok Katmanlı Aşırı Öğrenme Makinesi ve Rüzgar Hızı Tahmininde Kıyaslamalı Başarımı. *Kocaeli Üniversitesi Fen Bilimleri Dergisi, 3*(2), 147-153.

Kasun, L. L. C., Zhou, H., Huang, G.-B. vd. (2013). Representational learning with extreme learning machine for big data.

Kaur, R., Roul, R. K., & Batra, S. (2023). Multilayer extreme learning machine: a systematic review. *Multimedia Tools and Applications*, 1-39.

Klein, R. W., Temple, M. A., & Mendenhall, M. J. (2009). Application of wavelet-based RF fingerprinting to enhance wireless network security. *Journal of Communications and Networks, 11*(6), 544-555.

Kloc, M., Weigel, R., & Koelpin, A. (2017). SDR implementation of an adaptive low-latency IEEE 802.11 p transmitter system for real-time wireless applications. *2017 IEEE radio and wireless symposium (RWS)*, s. 207-210.

Köse, M., Taşcioğlu, S., & Telatar, Z. (2019). RF fingerprinting of IoT devices based on transient energy spectrum. *IEEE Access, 7*, 18715-18726.

Ktonas, P. Y., & Papp, N. (1980). Instantaneous envelope and phase extraction from real signals: theory, implementation, and an application to EEG analysis. *Signal Processing, 2*(4), 373-385.

Lan, Y., Soh, Y. C., & Huang, G.-B. (2009). A constructive enhancement for online sequential extreme learning machine. *2009 International Joint Conference on Neural Networks*, s. 1708-1713.

Liang, J.-H., Huang, Z.-T., & Li, Z.-W. (2017). Method of empirical mode decomposition in specific emitter identification. *Wireless Personal Communications, 96*(2), 2447-2461.

Liao, S., & Feng, C. (2014). Meta-ELM: ELM with ELM hidden nodes. *Neurocomputing, 128*, 81-87.

Lin, T.-Y., Lai, C.-M., & Chen, C.-W. USING SDR PLATFORM TO EXTRACT THE RF FINGERPRINT OF THE WIRELESS DEVICES FOR DEVICE IDENTIFICATION.

Lin, T.-Y., Lai, C.-M., & Chen, C.-W. (2020). Using SDR Platform to Extract the RF Fingerprint of the Wireless Devices for Device Identification. *CS & IT Conference Proceedings*

Lin, Y., Zhu, X., Zheng, Z. vd. (2019). The individual identification method of wireless device based on dimensionality reduction and machine learning. *The Journal of Supercomputing, 75*(6), 3010-3027.

Liu, Y., Wang, J., Niu, S. vd. (2021). ADS-B signals records for non-cryptographic identification and incremental learning. *IEEE, Piscataway, NJ, USA, Data Set*.

Liu, Y., Wang, J., Song, H. vd. (2020). A 24-hour signal recording dataset with labels for cybersecurity and IoT. *IEEE, Piscataway, NJ, USA, Data Set*.

Manjula, M., Mishra, S., & Sarma, A. (2013). Empirical mode decomposition with Hilbert transform for classification of voltage sag causes using probabilistic neural network. *International Journal of Electrical Power & Energy Systems, 44*(1), 597-603.

Merchant, K., Revay, S., Stantchev, G. vd. (2018). Deep learning for RF device fingerprinting in cognitive communication networks. *IEEE Journal of Selected Topics in Signal Processing, 12*(1), 160-167.

Miyashiro, H., Medrano, M., Huarcaya, J. vd. (2017). Software defined radio for hands-on communication theory. *2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, s. 1-4.

Moety, F. (2014). *Joint minimization of power and delay in wireless access networks.* Université Rennes 1.

Mohamed, I. S., Dalveren, Y., & Kara, A. (2020). Performance Assessment of Transient Signal Detection Methods and Superiority of Energy Criterion (EC) Method. *IEEE Access, 8*, 115613-115620.

Mohanti, S., Soltani, N., Sankhe, K. vd. (2020). AirID: Injecting a custom RF fingerprint for enhanced UAV identification using deep learning. *GLOBECOM 2020-2020 IEEE Global Communications Conference*, s. 1-6.

Nouichi, D., Abdelsalam, M., Nasir, Q. vd. (2019). Iot devices security using rf fingerprinting. *2019 Advances in Science and Engineering Technology International Conferences (ASET)*, s. 1-7.

Nyathi, T., & Ndlovu, S. Beacon Frame Manipulation to Mitigate Rogue Access Points: Case of Smartphone Rogue Access Points.

O'Shea, T. J., Roy, T., & Clancy, T. C. (2018). Over-the-air deep learning based radio signal classification. *IEEE Journal of Selected Topics in Signal Processing, 12*(1), 168-179.

Paillassa, B., & Morlet, C. (2003). Flexible satellites: software radio in the sky. *10th International Conference on Telecommunications, 2003. ICT 2003.*, s. 1596-1600.

Palamà, I., Gringoli, F., Bianchi, G. vd. (2021). IMSI Catchers in the wild: A real world 4G/5G assessment. *Computer Networks, 194*, 108137.

Park, J.-S., Yoon, H., & Jang, B.-J. (2016). SDR-based frequency interference analysis test-bed considering time domain characteristics of interferer. *2016 18th International Conference on Advanced Communication Technology (ICACT)*, s. 517-521.

Park, Y., Kuk, S., Kang, I. vd. (2016). Overcoming IoT language barriers using smartphone SDRs. *IEEE Transactions on Mobile Computing, 16*(3), 816-828.

Parmaksız, H., & Karakuzu, C. (2022a). Performance analysis of Extreme Learning Machine Classifiers on Radio Frequency Fingerprinting. *BSEU Engineering Research and Technology, 3*(2), 1-7.

Parmaksız, H., & Karakuzu, C. (2022b). Yazılım Tanımlı Radyoya Dayalı RF Parmak İzi Toplamak için Düşük Maliyetli Bir Çözüm. *Rahva Teknik ve Sosyal Araştırmalar Dergisi, 2*(2), 179-188.

Parvathi, G., & Basu, P. Analysis of RF Device Fingerprinting using Convolutional Neural Network.

Peng, L., Hu, A., Zhang, J. vd. (2018). Design of a hybrid RF fingerprint extraction and device classification scheme. *IEEE Internet of Things Journal, 6*(1), 349-360.

Peng, L., Zhang, J., Liu, M. vd. (2019). Deep learning based RF fingerprint identification using differential constellation trace figure. *IEEE Transactions on Vehicular Technology, 69*(1), 1091-1095.

Perotoni, M. B., & dos Santos, K. M. (2021). SDR-based spectrum analyzer based in open-source GNU radio. *Journal of Microwaves, Optoelectronics and Electromagnetic Applications, 20*, 542-555.

Picinbono, B. (1997). On instantaneous amplitude and phase of signals. *IEEE Transactions on signal processing, 45*(3), 552-560.

Pohl, J., & Noack, A. (2018). Universal radio hacker: A suite for analyzing and attacking stateful wireless protocols. *12th {USENIX} Workshop on Offensive Technologies ({WOOT} 18)*

Rahman, M. H., & Islam, M. M. (2016). A practical approach to spectrum analyzing unit using rtl-sdr. *Rajshahi University Journal of Science and Engineering, 44*, 151-159.

Rahman, M. M. U., Yasmeen, A., & Gross, J. (2014). Phy layer authentication via drifting oscillators. *2014 IEEE Global Communications Conference*, s. 716-721.

Rajendran, S., Meert, W., Giustiniano, D. vd. (2018). Deep learning models for wireless signal classification with distributed low-cost spectrum sensors. *IEEE Transactions on Cognitive Communications and Networking, 4*(3), 433-445.

Ramírez-Gallego, S., Lastra, I., Martínez-Rego, D. vd. (2017). Fast-mRMR: Fast minimum redundancy maximum relevance algorithm for high-dimensional big data. *International Journal of Intelligent Systems, 32*(2), 134-152.

Rao, C. R., & Mitra, S. K. (1972). Generalized inverse of a matrix and its applications. *Proceedings of the sixth Berkeley symposium on mathematical statistics and probability*, s. 601-620.

Ray, P. P. (2016). A survey of IoT cloud platforms. *Future Computing and Informatics Journal, 1*(1-2), 35-46.

Rehman, S. U., Alam, S., & Ardekani, I. T. (2014). An overview of radio frequency fingerprinting for low-end devices. *International Journal of Mobile Computing and Multimedia Communications (IJMCMC), 6*(3), 1-21.

Rehman, S. U., Sowerby, K., & Coghill, C. (2012). RF fingerprint extraction from the energy envelope of an instantaneous transient signal. *2012 Australian Communications Theory Workshop (AusCTW)*, s. 90-95.

Rehman, S. U., Sowerby, K. W., & Coghill, C. (2014). Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios. *IET communications, 8*(8), 1274-1284.

Reus-Muns, G., Jaisinghani, D., Sankhe, K. vd. (2020). Trust in 5G open RANs through machine learning: RF fingerprinting on the POWDER PAWR platform. *GLOBECOM 2020-2020 IEEE Global Communications Conference*, s. 1-6.

RF Wireless World (2023). *WLAN Beacon Frame.* [Erişim: 01.06.2023, https://www.rfwireless-world.com/Terminology/WLAN-beacon-frame.html]

Riyaz, S., Sankhe, K., Ioannidis, S. vd. (2018). Deep learning convolutional neural networks for radio identification. *IEEE Communications Magazine, 56*(9), 146-152.

Rong, H.-J., Ong, Y.-S., Tan, A.-H. vd. (2008). A fast pruned-extreme learning machine for classification problem. *Neurocomputing, 72*(1-3), 359-366.

RPi-3 Block Diagram (2023). *Raspberry Pi 3 Block Diagram Revision:4.* [Erişim: 12.07.2023, https://community.element14.com/products/raspberry-pi/b/blog/posts/raspberry-pi-3-block-diagram]

Sadowski, S., & Spachos, P. (2018). Rssi-based indoor localization with the internet of things. *IEEE Access, 6*, 30149-30161.

Samuel, J. N. (2018). *Specific emitter identification for GSM cellular telephones.* University of Pretoria.

Sankhe, K., Belgiovine, M., Zhou, F. vd. (2019). No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments. *IEEE Transactions on Cognitive Communications and Networking, 6*(1), 165-178.

Sankhe, K., Belgiovine, M., Zhou, F. vd. (2019). ORACLE: Optimized radio classification through convolutional neural networks. *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, s. 370-378.

Seo, J., Chen, Y.-H., De Lorenzo, D. S. vd. (2011). A real-time capable software-defined receiver using GPU for adaptive anti-jam GPS sensors. *Sensors, 11*(9), 8966-8991.

Sharaf Dabbagh, Y., & Saad, W. (2018). Authentication of Everything in the Internet of Things: Learning and Environmental Effects. *arXiv e-prints*, arXiv: 1805.00969.

Shen, G., Zhang, J., Marshall, A. vd. (2021). Radio frequency fingerprint identification for LoRa using spectrogram and CNN. *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*, s. 1-10.

Shen, G., Zhang, J., Marshall, A. vd. (2021). Radio frequency fingerprint identification for security in low-cost IoT devices. *2021 55th Asilomar Conference on Signals, Systems, and Computers*, s. 309-313.

Skorup, B. (2013). Reclaiming federal spectrum: Proposals and recommendations. *Colum. Sci. & Tech. L. Rev., 15*, 90.

Silicon Labs (2023). *Wi-Fi Coexistence*. [Erişim: 01.06.2023, https://www.silabs.com/wireless/wi-fi/wi-fi-coexistence]

Soltani, N., Reus-Muns, G., Salehi, B. vd. (2020). RF fingerprinting unmanned aerial vehicles with non-standard transmitter waveforms. *IEEE Transactions on Vehicular Technology, 69*(12), 15518-15531.

Soltani, S., Sagduyu, Y. E., Hasan, R. vd. (2019). Real-time and embedded deep learning on FPGA for RF signal classification. *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*, s. 1-6.

Soltanieh, N., Norouzi, Y., Yang, Y. vd. (2020). A review of radio frequency fingerprinting techniques. *IEEE Journal of Radio Frequency Identification, 4*(3), 222-233.

SourceForge (2023). *SDR Focused Distribution for the Raspberry Pi*. [Erişim: 01.06.2023, https://sourceforge.net/projects/dragonos-pi64/]

Sruthi, M., Abirami, M., Manikkoth, A. vd. (2013). Low cost digital transceiver design for Software Defined Radio using RTL-SDR. *2013 international mutli-conference on automation, computing, communication, control and compressed sensing (iMac4s)*, s. 852-855.

Stewart, R. W., Barlee, K. W., Atkinson, D. S. vd. (2015). *Software defined radio using MATLAB & Simulink and the RTL-SDR*. Strathclyde Academic Media.

Sun, X., & Ansari, N. (2016). EdgeIoT: Mobile edge computing for the Internet of Things. *IEEE Communications Magazine, 54*(12), 22-29.

Suski II, W. C., Temple, M. A., Mendenhall, M. J. vd. (2008). Using spectral fingerprints to improve wireless network security. *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*, s. 1-5.

Süzen, A. A., Duman, B., & Şen, B. (2020). Benchmark analysis of jetson tx2, jetson nano and raspberry pi using deep-cnn. *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, s. 1-5.

TajDini, M., Sokolov, V., & Buriachok, V. (2019). Men-in-the-middle attack simulation on low energy wireless devices using software define radio. *Available at SSRN 3455453*.

Tang, J., Deng, C., & Huang, G.-B. (2015). Extreme learning machine for multilayer perceptron. *IEEE transactions on neural networks and learning systems, 27*(4), 809-821.

Tang, J., Deng, C., Huang, G.-B. vd. (2014). Compressed-domain ship detection on spaceborne optical image using deep neural network and extreme learning machine. *IEEE transactions on geoscience and remote sensing, 53*(3), 1174-1185.

Taşcıoğlu, S., Köse, M., & Soysal, G. (2022). Sequential Transient Detection for RF Fingerprinting. *Electronics, 11*(20), 3333.

Taşcıoğlu, S., Köse, M., & Telatar, Z. (2017). Effect of sampling rate on transient based RF fingerprinting. *2017 10th International Conference on Electrical and Electronics Engineering (ELECO)*, s. 1156-1160.

Tiwari, P., Singh, N., Dixit, A. vd. (2014). Multivariate sequence analysis reveals additional function impacting residues in the SDR superfamily. *Proteins: Structure, Function, and Bioinformatics, 82*(10), 2842-2856.

Tme Eu (2023). *ANT-DB1-LCD-CCC Data Sheet.* [Erişim: 01.06.2023, https://www.tme.eu/Document/6e10b54d2a246213f9dac56a794a9a0b/ant-db1-lcd-ccc-data-sheet.pdf]

Ureten, O., & Serinken, N. (2007). Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering, 32*(1), 27-33.

Uzundurukan, E., Dalveren, Y., & Kara, A. (2020). A database for the radio frequency fingerprinting of Bluetooth devices. *Data, 5*(2), 55.

Vo-Huu, T. D., Vo-Huu, T. D., & Noubir, G. (2016). Fingerprinting Wi-Fi devices using software defined radios. *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, s. 3-14.

Wong, C. M., Vong, C. M., Wong, P. K. vd. (2016). Kernel-based multilayer extreme learning machines for representation learning. *IEEE transactions on neural networks and learning systems, 29*(3), 757-762.

Woodings, R. W., & Gerrior, M. (2005). Avoiding interference in the 2.4-GHz ISM band. *Microwave Engineering Online*.

Wu, Q., Feres, C., Kuzmenko, D. vd. (2018). Deep learning based RF fingerprinting for device identification and wireless security. *Electronics Letters, 54*(24), 1405-1407.

Xiong, X., Xiang, W., Zheng, K. vd. (2015). An open source SDR-based NOMA system for 5G networks. *IEEE Wireless Communications, 22*(6), 24-32.

Xu, C., Chen, B., Liu, Y. vd. (2020). RF fingerprint measurement for detecting multiple amateur drones based on STFT and feature reduction. *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*, s. 4G1-1-4G1-7.

Xu, T., & Darwazeh, I. (2020). Deep learning for over-the-air non-orthogonal signal classification. *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, s. 1-5.

Yu, D., & Deng, L. (2012). Efficient and effective algorithms for training single-hidden-layer neural networks. *Pattern recognition letters, 33*(5), 554-558.

Yu, J., Hu, A., Zhou, F. vd. (2019). Radio frequency fingerprint identification based on denoising autoencoders. *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, s. 1-6.

Yuan, Y., Huang, Z., Wu, H. vd. (2014). Specific emitter identification based on Hilbert-Huang transform-based time-frequency-energy distribution features. *IET communications, 8*(13), 2404-2412.

Zhang, J., Duong, T. Q., Marshall, A. vd. (2016). Key generation from wireless channels: A review. *IEEE Access, 4*, 614-626.

Zhang, J., Rajendran, S., Sun, Z. vd. (2019). Physical layer security for the Internet of Things: Authentication and key generation. *IEEE Wireless Communications, 26*(5), 92-98.

Zhang, J., Xu, Z., Li, J. vd. (2023). Wi-Fi device identification based on multi-domain physical layer fingerprint. *Computer Communications, 204*, 118-129.

Zhou, J., Zhang, X., Xiong, E. vd. (2016). SDR-recycling signal amplification for highly sensitive methyltransferase activity assay. *Journal of Electroanalytical Chemistry, 781*, 304-309.

Zhu, Q.-Y., Qin, A. K., Suganthan, P. N. vd. (2005). Evolutionary extreme learning machine. *Pattern recognition, 38*(10), 1759-1763.

Zhu, W., Miao, J., & Qing, L. (2015). Constrained extreme learning machines: A study on classification cases. *arXiv preprint arXiv:1501.06115*.

Ziegler, J. L., Arn, R. T., & Chambers, W. (2017). Modulation recognition with GNU radio, keras, and HackRF. *2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, s. 1-3.

Zong, L., Xu, C., & Yuan, H. (2020). A rf fingerprint recognition method based on deeply convolutional neural network. *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)*, s. 1778-1781.