GPS Tabanlı Konum Belirleme Sistemlerinin Güvenliği ve Sinyal Geliş Doğrultusu Kestirimi ile Saldırı Tespiti

Bu tez Bilgi Güvenliği Mühendisliği'nde
Tezli Yüksek Lisans Programının bir koşulu olarak

Mustafa Haki KOZAN
tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.

İSTANBUL
ŞEHİR
ÜNİVERSİTESİ

Bu tezi okuduk, kapsam ve nitelik açısından Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans derecesi için tümüyle uygun olduğu görüşüne vardık.

ONAYLAYANLAR:

Prof. Dr. Ensar GÜL
(Tez Danışmanı) .....

Dr.İbrahim HÖKELEK
(Tez Eş-danışmanı) .....

Doç. Dr. Ali Fuat ALKAYA .....

Dr. Öğretim Üyesi Mehmet Serkan APAYDIN .....

Bu tez İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü tarafından belirlenen tüm koşullara uygundur.

ONAY TARİHİ: 27.08.2019

MÜHÜR/İMZA:

Yazarlık Beyanı

Ben, Mustafa Haki KOZAN, başlığı, 'GPS Tabanlı Konum Belirleme Sistemlerinin Güvenliği ve Sinyal Geliş Doğrultusu Kestirimi ile Saldırı Tespiti' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza: 

Tarih: 27.08.2019

"Bilgi bilgelik değildir."

Albert Einstein

GPS Tabanlı Konum Belirleme Sistemlerinin Güvenliği ve Sinyal Geliş Doğrultusu Kestirimi ile Saldırı Tespiti

Mustafa Haki KOZAN

Öz

Bu tez kapsamında GPS sinyal karıştırıcı ve GPS aldatma saldırılarının tespiti amacıyla çoklu kaynaktan yapılan karmaşık saldırıları daha hassas tespit etmeye yönelik sinyal geliş doğrultusu (DOA-Direction of Arrival) tabanlı saldırı tespit yöntemi üzerine çalışılmıştır. Yöntem literatürde yaygın olarak kullanılan MUSIC, Root-MUSIC, ESPRIT, CAPON DOA algoritmalarının GPS sinyalinin ve aldatma saldırılarının karakteristik özelliklerine göre parametre optimizasyonu ile gerçekleştirilmiştir. Gerçek hayattaki saldırılarda GPS aldatma sinyalleri çoğunlukla tek bir kaynaktan üretilir. Bu yöntemdeki parametre optimizasyonu gerçek GPS uydularından alınan farklı noktalardaki uydu konum ve açı bilgileriyle tek kaynaktan gelen aldatma sinyallerinin farkı gözönüne alınarak saldırı tespiti gerçekleştirilmiştir. Tez kapsamında önerilen yöntemin başarım analizi MATLAB simülasyon aracı kullanılarak yapılmıştır. Simülasyon senaryolarını oluşturmak için GPS uydularından alınan gerçek GPS sinyal örneklerine ilave olarak yapay olarak oluşturulan sanal aldatma sinyalleri kullanılmıştır.Simülasyon sonuçları DOA algoritmalarında kullanılan parametrelerin uygun seçiminin başarım performansını önemli derecede etkilediğini göstermektedir.

Anahtar Sözcükler: Bilgi Güvenliği, Konum Belirleme, GPS, Uydu Haberleşmesi, Aldatma Saldırıları ve Tespiti, Sinyal Geliş Doğrultusu (DOA-Direction of Arrival)

Security of GPS Based Positioning Systems and Spoofing Detection with Direction of Arrival

Mustafa Haki KOZAN

Abstract

In this thesis, we propose a new GPS signal jamming and spoofing attack detection method based on DOA (Direction of Arrival) which can handle more complex attack scenarios from multiple sources. For this purpose, the heavily used GPS signal jamming and spoofing attack detection methods in literature, namely MUSIC, Root-MUSIC, ESPRIT, CAPON DOA are analyzed and the parameters of these methods that can optimize the performance are identified according the characteristics of the attack scenarios. In real-life attacks, GPS spoofing signals are often generated from a single source. The parameter optimization in the proposed method is based on the difference between the satellite position and angle information obtained from the real GPS satellites and multiple spoofing signals. The performance analysis of the proposed method has been done using the MATLAB simulation tool. Artificial virtual spoofing signals are used to generate simulation scenarios in addition to the actual GPS signal samples received from real GPS satellites. Simulation results show that the proper selection of the parameters used in the DOA algorithms significantly affect the performance.

Keywords: Information Security, Geolocation, GPS, Satellite Communication, Spoofing Attacks and Detection, DOA-Direction of Arrival

Sevgili Aileme

Teşekkür

Tez çalışmalarım boyunca desteklerinden dolayı danışmanım Prof.Dr.Ensar GÜL'e, çalıştığım kurum TÜBİTAK BİLGEM'e, Dr.Serdar Özgür ATA'ya ve Dr.İbrahim HÖKELEK'e çok teşekkür ederim.

İçindekiler

Şekil Listesi

Tablo Listesi

Kısaltmalar

ADC	**A**nalog to **D**igital **C**onverter
AGC	**A**utomatic **G**ain **C**ontroller
A-GPS	**A**ssisted **G**PS
AIS	**A**utomatic **I**dentification **S**ystem
APD	**A**utocorrelation **P**eak **D**istortion
ANS	**A**daptable **N**avigation **S**ystems
BKZS	**B**ölgesel **K**onumlama ve **Z**amanlama **S**istemi
BTK	**B**ilgi **T**eknolojileri ve **İ**letişim **K**urulu
CLT	**C**entral **L**imit **T**heorem
CNR	**C**arrier **N**oise **R**atio
CRC	**C**yclic **R**edundancy **C**heck
CRPA	**C**ontrolled **R**adiated **P**attern **A**ntenna
DARPA	**D**efense **A**dvanced **R**esearch **P**rojects **A**gency
D-GPS	**D**ifferantial **G**PS
DOA	**D**irection **o**f **A**rrival
DSN	**D**eep **S**pace **N**etwork
ELORAN	**E**nhanced **L**ong **RA**nge **N**avigation
EGNOS	**E**uropean **G**eostationary **N**avigation **O**verlay **S**ervice
ESPRIT	**E**stimation of **S**ignal **P**arameters via rotational **I**nvariance **T**echniques
GAJT	**G**PS **A**nti **J**am **T**echnology
GLONASS	**GLO**balnaya **NA**vigatsionnaya **S**putnikovaya
GPS	**G**lobal **P**ositioning **S**ystem
GAGAN	**G**PS **A**ided **G**EO **A**ugmented **N**avigation
GNSS	**G**lobal **N**avigation **S**atellite **S**ystems
GSM	**G**lobal **S**ystem for **M**obile

IF	**I**ntermediate **F**requecy
INS	**I**nertial **N**avigation **S**ystem
IRNSS	**I**ndian **R**egional **N**avigation **S**atellite **S**ystem
KLIF	**K**ey Data Processor **L**oading and **I**nstallation **F**acility
LORAN	**LO**ng **RA**nge **N**avigation
MSAS	**M**TSAT **S**atellite **A**ugmentation **S**ystem
MUSIC	**MU**ltiple **SI**gnal **C**lassification
NASA	**N**ational **A**eronautics and **S**pace **A**dministration
NMEA	**N**ational **M**arine **E**lectronics **A**ssociation
OTAD	**O**ver **T**he **A**ir **D**istribution
PRN	**P**seudo **R**andom **N**oise
RF	**R**adio **F**requecy
RTK	**R**eal **T**ime **K**inematic
SAASM	**S**elective **A**vailability **A**nti **S**poofing **M**odule
SAW	**S**urface **A**coustic **W**ave
SLAM	**S**imultaneous **L**ocalization **A**nd **M**apping
SLC	**S**ide **L**obe **C**ancellation
SQM	**S**ignal **M**ount **T**echnology
SMT	**S**urface **R**andom **N**oise
SNR	**S**ignal to **N**oise **R**atio
STL	**S**atellite **T**ime and **L**ocation
TCK	**T**ürk **C**eza **K**anunu
TUSAG	**T**ürkiye **U**lusal **SA**bit **G**PS İstasyonu **A**ğı
UAV	**U**nmanned **A**erial **V**ehicle
UHF	**U**ltra **H**igh **F**requency
ULA	**U**niform **L**inear **A**rray
USRP	**U**niversal **S**oftware **R**adio **P**eripheral
WAAS	**W**ide **A**rea **A**ugmentation **S**ystem

Bölüm 1

Giriş

1.1 GPS Sistemlerine Giriş

GPS küresel uydu seyrüsefer sistemlerinin en aktif kullanılan ve eski örneğidir. 1978 yılından itibaren Amerikan Savunma Bakanlığı tarafından kurulmuş ve işletilmektedir. Dünyanın çevresine atılan 24 adet aktif uydu ve yedeklerle birlikte 32 uydudan oluşan bir sistemdir. Hayatın vazgeçilmez bir parçası haline gelen GPS sisteminin mevcut yapısının güvenlik açıkları ve riskleri bu sistem üzerine yapılan çalışmalarla minimize edilmiştir. Güvenli haberleşmenin temeli gizlilik, erişilebilirlik ve bütünlüğe dayanır. Bu temeller doğrultusunda GPS sisteminden istenen güvenlik kriterleri; mesaj içeriğinin gizli olarak elde edilmesi, haberleşme kanalının her zaman ulaşabilir kalması ve gönderilen mesajın tam ve değişmemiş olarak karşıya ulaştırarak bütünlüğün korunmasıdır. Güvenli haberleşmenin istenen bu güvenlik kriterleri temel alınarak GPS sisteminin sorunları araştırıldı ve bu sorunların çözümleri incelendi [3].

GPS üzerinden yapılan saldırılar GPS sinyal karıştırma ve GPS aldatma olarak iki ana sınıfa ayrılabilir. Literatürdeki çözümler incelendiğinde her iki saldırının tespiti için uygulanabilen GPS sinyal geliş doğrultusu (DOA) tabanlı saldırı tespit yöntemi bu tezde kullanıldı. GPS uyduları üzerinden, uydulara ait efemeris veriler belli sıklıklarla yayınlanır. GPS alıcılarında bu GPS uydu konum verileri vardır. GPS uydularının herbiri kendi orbital yörüngesinde birbirinden çok farklı ve önceden bilinen konumlardan yayın yapmaktadır. Tipik bir aldatma saldırısında ise tüm uydu yayınları tek yönden gelmektedir ve tez kapsamında geliştirilen saldırı tespit yönteminde bu farklılık gözönüne alınmıştır.

DOA algoritmalarının uygulamasında anten sayısı, anten dizilimi, örnekleme sayısı, sinyal kuvveti gibi parametreler algoritmanın başarısını etkilemektedir. MUSIC, Root-MUSIC, ESPRIT, CAPON yöntemleri başlıca DOA tespit algoritmalarıdır. Bu algoritmaların başarım analizlerinin yapıldığı MATLAB simülasyon çalışmasında gerçek GPS verileri kullanılmıştır. Bu verilerden uydulara ait açı verileri alınmış sonra sanal GPS aldatma sinyalleri eklenip bu sinyallerin DOA tespitini bahsedilen 4 farklı algoritma kullanılarak en verimli GPS aldatma tespit algoritmasının bulunmasına çalışılmıştır.

Tezin amacı kapsamında önceki DOA ile GPS aldatma saldırısı tespiti çalışmalarına göre daha kompleks saldırılar ve çoklu aldatma kaynağı kullanımı durumunda daha başarılı çözümler bulmak hedeflenmektedir. Gerçek ve saldırgan kaynakların çok yakın olması gibi zorluklarda ve çok daha hassas açıda yön bulmak gerektiğinde yeni yöntemlere ihtiyaç vardır. Bu tezde de çok daha hassas konum açıları bulunması amaçlanır.

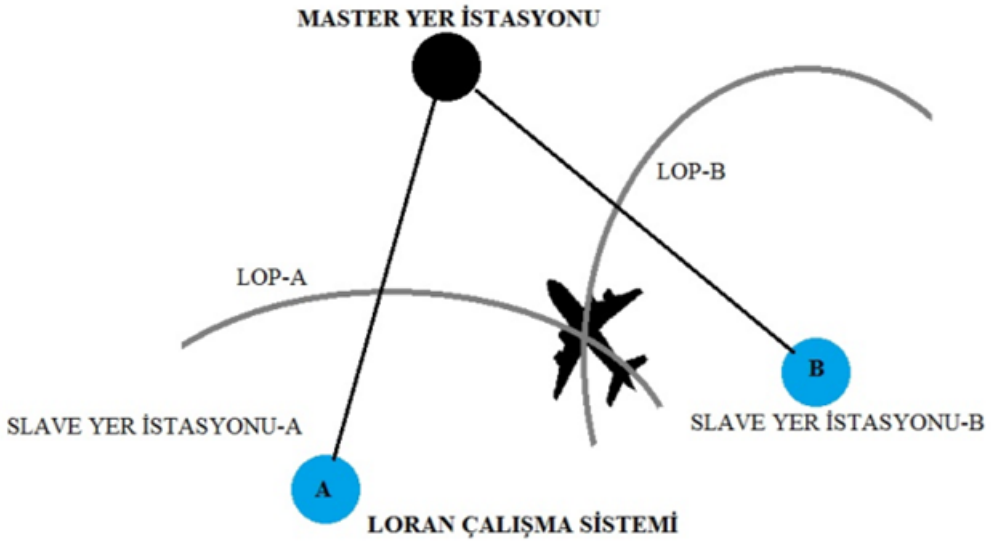
Bu tezin içeriği altı bölümde anlatılmıştır. Birinci bölümde tezin içeriği ve kapsamı hakkında bilgi verilmiştir. İkinci bölümde GPS sisteminin geçmişi, temelleri, matematiksel altyapısı ve benzer konumlama sistemleri anlatılmıştır. Askeri ve sivil GPS kullanım farklılıkları, askeri GPS sistemindeki güvenlik önlemleri ve anahtar değişimi konuları işlenmiştir. Üçüncü bölümde tarihte gerçekleşmiş GPS saldırıları, GPS aldatma ve GPS sinyal karıştırma saldırı çeşitleri, saldırı yapılış metotları ve bunlara karşı alınan önlemler çözümler altında anlatılmıştır. Dördüncü bölümde GPS sinyal karıştırıcı ve GPS aldatma saldırılarının tespitinde kullanabileceğimiz DOA yöntemleri hakkında bilgi verilmiştir ve bu konu ile ilgili literatürdeki çalışmalar sunulmuştur. Beşinci bölümde tez kapsamında önerilen yöntemin başarım analizi MATLAB simülasyon aracı kullanılarak yapılmıştır. Bu doğrultuda simülasyon senaryolarını oluşturmak için GPS uydularından alınan gerçek GPS sinyal örneklerine ilave olarak yapay olarak sanal aldatma sinyalleri oluşturulmuştur. Altıncı bölümde tez kapsamında yapılan çalışmalar ve önemli sonuçlar özetlenmiştir.

Bölüm 2

Konumlama Sistemleri

2.1 Konumlama Sistemlerine Giriş

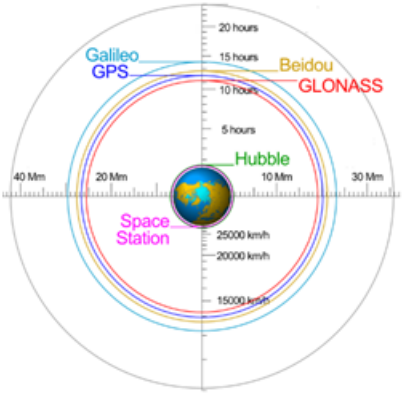
İnsanoğlu yeryüzünde var olduğundan itibaren çevresini merak etmiş ve bu merakı sonucunda yolculuklar yapıp çevresini tanımıştır. Konum ve yön bulmayı güneş, ay, yıldızlar kullanarak yapmış sonrasında haritalar, deniz fenerleri ve pusulalar kullanılmıştır. Küresel bazlı konum belirleme sistemi olarak ilk çalışmalar radyo dalgası üzerinden karasal sinyallerle yapılan konum hesaplama tabanlı sistemlerdir. DECCA, OMEGA ve LORAN bu sistemin önemli örnekleridir. LORAN ise karasal sistemlerin en çok kullanılanıdır. LORAN 2. Dünya Savaşı sırasında ABD tarafından geliştirilen temeli ingilizlerin GEE sistemiyle aynı olan gemiler ve hava araçlarının konum belirlemesi için kullanılan sistemidir. Bu sistemde Şekil 2.1'de anlatıldığı gibi kıyılara konular istasyonlardan 100 kHz de senkronize şekilde RF sinyaller üretilir. Bu mesajı alan alıcı farklı istasyonlardan gelen mesajların geliş zaman farkından kendi konumunu bulmaya çalışır. 2. Dünya Savaşı'nda %30 Soğuk Savaş'ın sonunda da %70 civarında küresel kapsama alanına ulaşmıştır. 70.000'den fazla alıcı, uçaklar ve gemiler için üretilmiştir [4]. Burada operasyon mesafesi çok azdır, atmosferik hata oranları yüksektir, yıllar içinde çokça versiyon ve gelişme olsa da hata oranı 200 metrenin altına inememiştir. ELORAN gibi hala aktif olarak kullanıldığı versiyonları vardır.



Şekil 2.1: LORAN Çalışma Prensibi [5]

2.2 GNSS Sistemi (Küresel Uydu Seyrüsefer Sistemi)

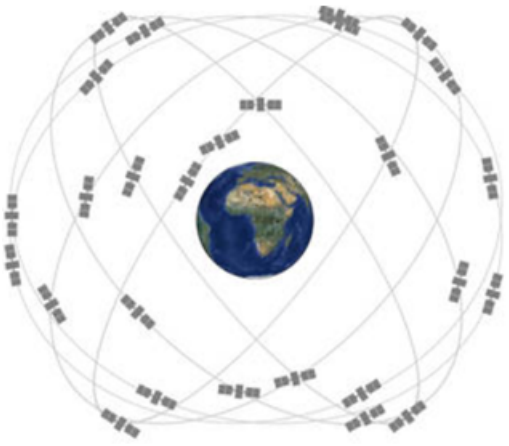
GNSS sistemleri uydu tabanlı konum belirleme sistemleridir. Daha önceleri karasal çözümlerle konum belirleme yapılmıştır ama coğrafi engeller, kapsama problemleri konumlamanın uzaydan yapılmasını zorunlu kılmıştır. NASA'nın DSN (Deep Space Network) projesi ile Sovyetler'in Sputnik uydusunun başarılı bir şekilde uzaya gönderilmesiyle uzay çağı başlamış ve GNSS sistemleri başta GPS olmak üzere geliştirilmiştir [6]. Şekil 2.2'de tüm GNSS uydu orbitalleri gösterilmiştir.



Şekil 2.2: GNSS Konum Haritası [7]

2.3 GPS Sistemi

GPS, GNSS (Global Navigation Satellite Systems -Küresel Uydu Seyrüsefer Sistemi) sistemlerinin en bilinen örneğidir. GPS Küresel konumlama sistemi Amerikan Savunma Bakanlığı tarafından 1978 yılından itibaren kurulan ve işletilen önceleri sadece askeri kullanımda olan sonra sivil kullanıma da açılmış olan bir sistemdir. Soğuk savaşın aktif olduğu 1983 yılında HL7442 nolu Güney Kore Havayolları'na ait yolcu uçağının Sovyet Hava Kuvvetleri tarafından hava sahası ihlali nedeniyle düşürülmesinin gerçekleşmesi GPS sisteminin sivil kullanımına açılmasını tetiklemiştir. Sivil kullanımda kısıtlamaların büyük bir çoğunluğu da 2000 yılından itibaren kaldırılmıştır [8]. Avrupa merkezli GALILEO, Rusya merkezli GLONASS, Hindistan merkezli IRNSS ve Çin merkezli COMPASS sisteminden çok daha önce geliştirilmiş ve küresel bazda en aktif kullanılan GNSS sistemidir [6]. Dünyanın çevresindeki Şekil 2.3'de gösterildiği gibi 6 yörünge üzerinde hareketlerini yapan 24 adet aktif uydu ve yedeklerle birlikte 32 uydudan oluşan bir sistemdir. GPS sisteminin çalışma temeli GPS uydularından yayılan üzerinde konum ve saat bilgisini içeren verinin GPS alıcısı tarafından alınıp GPS uydularına olan uzaklıklarının hesaplaması ve bu uzaklık hesaplarından da kendi konumunu 3 boyutlu olarak bulması üzerine dayanır. Bu hesaplamalarla alıcı konum, hız, zaman bilgisine ulaşır. GPS sisteminin başarılarından biri de çok zayıf bir sinyal (10^{-16} W) ile çok hassasiyette konum belirleyebilmesidir.



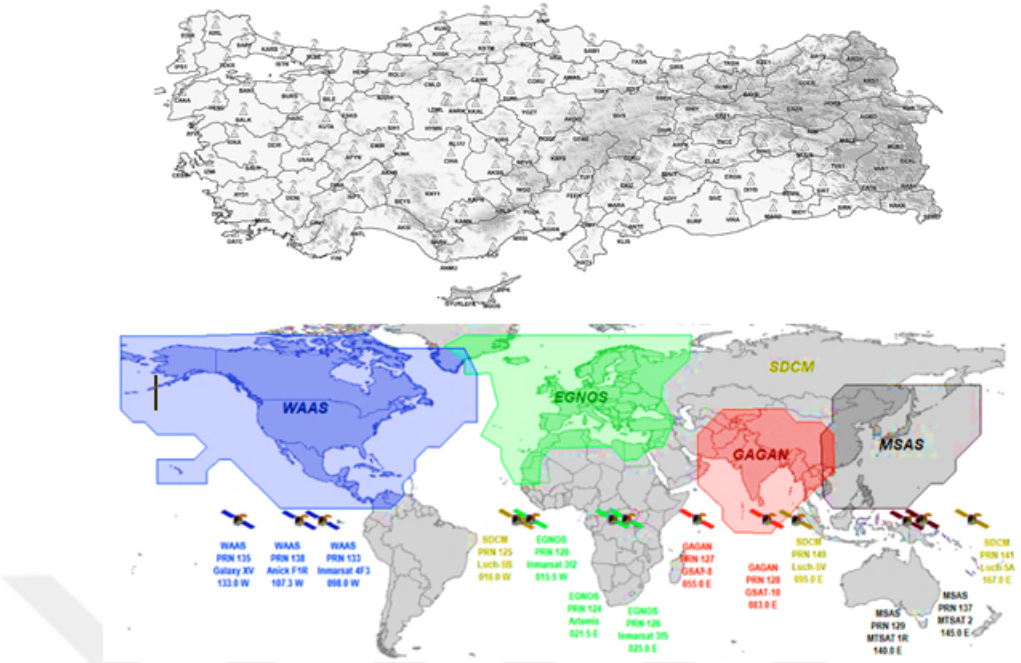
Şekil 2.3: GPS Uydularının Konumu [9]

2.4 GLONASS, GALILEO ve BEIDOU

GPS sisteminden başka kullanılan aktif GNSS sistemleri GLONASS, GALILEO ve COMPASS'dır. GLONASS Sovyetler Birliği zamanında başlayan bir projedir ve Sovyetler Birliğinin uzay projelerinin en büyük bütçelisidir. 2001'de tekrar çalışmalar hızlanıp 2011'de küresel ölçekte kapsama alanına erişmiştir [6]. Sivil ve askeri kullanımı vardır ve hassasiyette GPS'den daha iyidir. GALILEO, ABD kontrolündeki GPS ve Rusya kontrolündeki GLONASS'a karşı Avrupa Birliği tarafından desteklenen bir projedir. Küresel ölçekte kapsama alanı hedeflenmiştir ve ilk uydu 2005'de gönderilmiştir. 30 uydudan oluşan projenin 2019 yılında tam operasyona geçmesi beklenmektedir. Tüm uydular devreye girmesiyle GPS'den çok daha hassas GNSS sistemine erişmiş olunacaktır. Sivil, ticari ve askeri kullanımı vardır [6]. COMPASS (BEIDOU) 2000 yılında bölgesel ölçekli konumlama sistemi olarak başlayan, Çin tarafından geliştirilen ve 2020 yılında 35 uyduyla küresel ölçekte hizmet vermesi planlanan projesidir.
Konumlama sistemleri olarak Türkiye'de ise yapılan çalışma ilk olarak 2015 yılında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nca duyurulan sonra Savunma Sanayi Müsteşarlığı'nın projelendirdiği BKSZ (Bölgesel Konumlama ve Zamanlama Sistemi) sistemidir. Toplamda 6 uydunun yörüngeye oturtulması ile hayata geçirilmesi planlanan BKSZ sistemi ile GPS bölgesel konumlama sistemine kavuşacaktır ve sistemin en erken 2025'te hizmete girmesi planlanmaktadır.

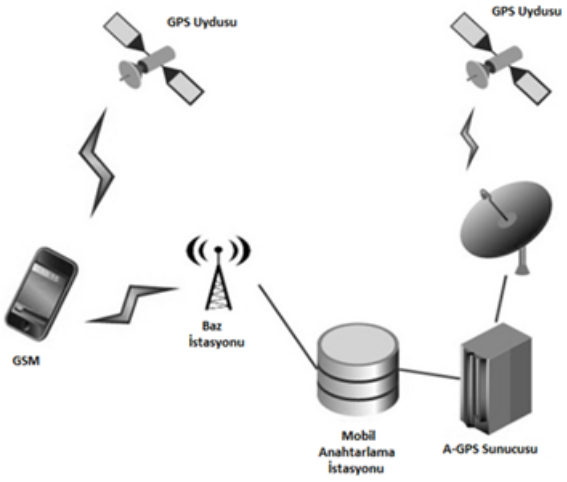
2.5 D-GPS ve A-GPS

GPS sistemi hesaplama hatası, atmosferik olaylar, zaman hataları gibi nedenlerle yüzlerce metreye kadar çıkabilir. D-GPS temeli karasal sabit referans istasyonlarla GPS sisteminin hatalarının düzeltilmesidir. 283.5 kHz - 2.95 MHz frekanslarında yayın yapılır. WAAS Kuzey Amerika merkezli, EGNOS Avrupa merkezli, GAGAN Hindistan merkezli, MSAS ise Japonya merkezli D-GPS yapılarıdır [10]. Türkiye'de ise Türkiye Ulusal Sabit GPS İstasyonları Ağı (TUSAGA)'dıyla ilk olarak Harita Genel Komutanlığı Sefik Erensü kışlasında kurulmuştur ve Şekil 2.4'de gösterildiği gibi şu an 146 adet aktif sabit GPS referans noktası vardır [11].



Şekil 2.4: Türkiye'de ve Küresel Ölçekte D-GPS [10],[11]

A-GPS: GPS sinyalin zayıf olduğu ve konum doğrulamasının yapılması gerektiği durumlarda kullanılmak için geliştirilmiştir. Hava durumları, fiziksel engeller ve kapalı ortamlar sinyal erişimini engeller. A-GPS GSM üzerinden Şekil 2.5'deki gibi baz istasyonları vasıtasıyla konum belirlemek için geliştirilmiştir. Sadece GSM üzerinden konum hesaplanırsa hata payı yüksektir ama A-GPS verisi bir back up verisi olarak GPS aldatma saldırısı tespitinde kullanılır [12].



Şekil 2.5: A-GPS Çalışma Prensibi [12]

2.6 GNSS Sinyal Yapıları

GPS uyduları 2 tür sinyal üretmektedir: Askeri M kod frekans bandı ve sivil L1,L2 frekans bandıdır. Sivil ve ticaride kullanılan L1,L2 frekans bandı şifreli değildir ve saldırılara açıktır, M kod frekansı ise şifrelidir ve askeri uygulamalarda kullanılmaktadır. GPS sivil ve ticari pek çok uygulamada kullanılmaktadır. Konumlama, takip, güvenlik gibi güncel kullanımı dışında zaman bilgisine erişimde de yararlanılmaktadır. Özellikle finansal işlemler, yayıncılık ve mobil iletişimde GPS zaman bilgisi kullanılmaktadır. GLONASS'da da GPS gibi 2 çeşit sinyalleşme vardır: Sivil frekansda şifresiz ve askeri frekansda şifreli yayın yapılmaktadır. GALILEO'da birkaç çeşit kullanım vardır. Sivil frekansı kullanım şifresiz ve herkese açıktır, ticari ve kamu kuruluşlarının kullandığı frekans ise şifrelidir [13]. Çok daha hassas ve sınırlı olan bu frekansın kullanımı için ücret ödenir.

2.7 GPS Çalışma Mantığı

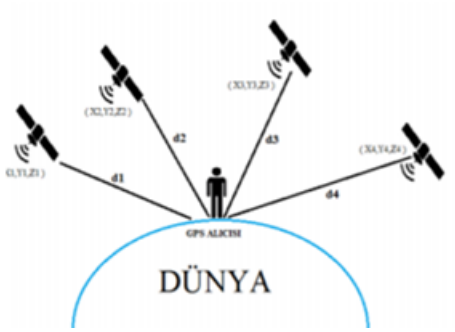
GPS haberleşmesi GPS uydu ve alıcı ikilisinden oluşur. Uydudan GPS sinyalleri yeryüzüne gönderilir, GPS alıcısı anten vasıtasıyla bu sinyalleri alır ve konum hesaplaması yapar. GPS uydularının kontrolü yeryüzünde farklı konumlarda olan komuta merkezlerinden olur. GPS çalışma sisteminde her uydu kendine ait ID kodu, konumu, zaman bilgisi ve diğer ilgili parametreleri gönderir. Alıcı da aldığı sinyalden hangi uydudan ve ne kadar sürede aldığına bakar sonra bu sinyalin taşıma hızını hesaplar ve zaman bilgisini de kullanarak uydulara olan uzaklıklarını hesaplar. (2.1)-(2.4)'deki denklemler kullanılarak en az dört uyduya olan uzaklıklar bulunur. d1, d2, d3, d4 GPS uydusundan alıcıya kadarki yolu ifade etmektedir ve hesaplama ışık hızında sinyalin aldığı yol üzerinden hesaplanmaktadır. ciB ise alıcının saatindeki ofset üzerinden hesaplana uzaklık farkını ifade eder. Bu denklemlerden x,y,z koordinatları hesaplanır. Bu hesaplamalar sonucu Şekil 2.6'deki üçgenlemeye (triangulation) yöntemleri ile alıcı kendi konumunu bulur [14].

$$d_1 = \sqrt{(x - x_1)^2 + (y - y_1)^2 + (z - z_1)^2} + ci_B \tag{2.1}$$

$$d_2 = \sqrt{(x - x_2)^2 + (y - y_2)^2 + (z - z_2)^2} + ci_B \tag{2.2}$$

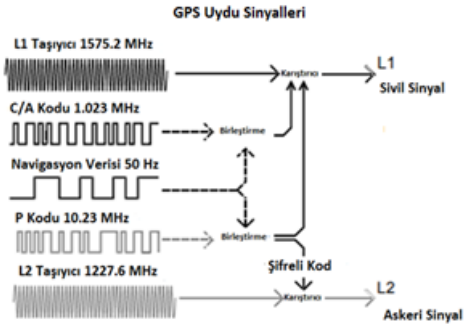
$$d_3 = \sqrt{(x - x_3)^2 + (y - y_3)^2 + (z - z_3)^2} + ci_B \tag{2.3}$$

$$d_4 = \sqrt{(x - x_4)^2 + (y - y_4)^2 + (z - z_4)^2} + ci_B \tag{2.4}$$



Şekil 2.6: GPS Çalışma Mantığı ve Matematiksel Hesaplaması [14]

Ekstra sensör verileri, Multi GNSS alıcısı kullanımı, D-GPS, A-GPS gibi araçları da kullanılarak maksimum doğrulukta konumlama yapılır. GPS'de doğruluk oranı beş metre altındadır ve bu oran ekstra doğrulamalarla iki,üç metrelere kadar düşürülür. Tüm GPS uyduları GPS sinyali 1575.2MHz L1 taşıyıcı frekansı ve 1227.6 MHz L2 taşıyıcı frekansı ile taşır. İki taşıyıcı frekansın kullanılmasının nedeni iyonosforik hatanın giderilmesidir. 1.023 MHz'lik C/A kodu her uydu için eşsiz olan kodu belirtmektedir. Bu bilgi ile GPS alıcısı hangi uydudan bilgi aldığını bilmektedir. 50 Hz ise konum ve tarih bilgisinin olduğu frekanstır [3]. Her uydu 1 milisaniyede kendi C/A kodunu yayınlar. GPS alıcısı da aynı ilk sinyali aldıktan sonra kendisi de içinde bu sinyali oluşturur ve aldığı sinyal ile oluşturduğu sinyal arasındaki gecikmeden uzaklığı hesaplar. P Kodu ise 10.23 MHz de 266 günde bir kendini tekrar eden GPS uydularının haftalık PRN ID'lerini yaydıkları frekanstır [15].



Şekil 2.7: GPS Sinyal Yapıları [16]

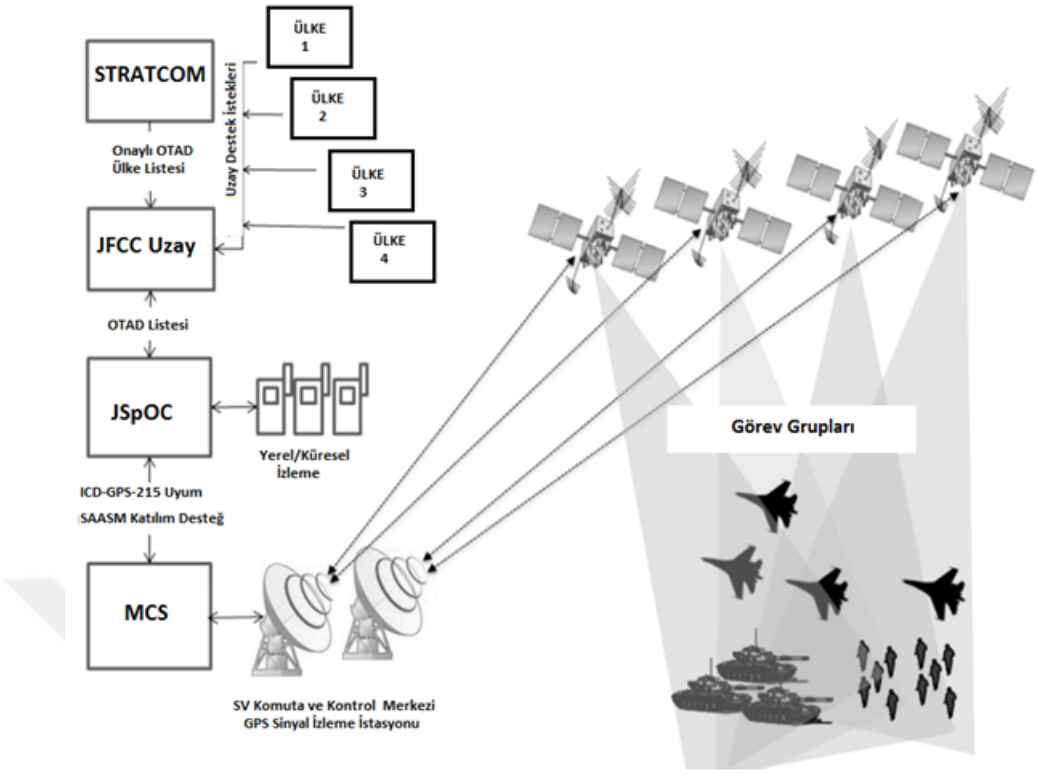
2.8 GPS Uydusu ve GPS Alıcısı

İlk GPS uydusu OPS 5111 1978'de uzaya gönderilmiştir ve yeryüzünden 20.000 km uzakta günde iki tam dünya turu yaparak yayın yapmaya başlamıştır. GPS sistemi dünyanın hemen hemen her yerinden en az altı uyduyu görecek şekilde konumlandırılmıştır. Ana yer kontrol merkezi Schriever Hava Üssü Colorado olmak üzere dünyanın dört bir yanında yedek kontrol ve izleme istasyonları vardır. Buradan uydularının güncellemeleri, kontrolleri ve almanak yüklemeleri yapılır [17]. GPS alıcıları GPS uydularından iki mesaj alır: Almanak ve efemeris. Almanak uyduların durumu ve yörüngeleri hakkında bilgi içerir. GPS alıcısı, hangi uyduların halihazırda görünür olduğunu hesaplamak için almanak kullanır. GPS alıcısı ilk kez kullanılacaksa veya bir süredir kullanılmamışsa, geçerli bir almanak verisinin elde edilmesi 15 dakikayı bulur. Efemeris verileri ise her uydunun yörüngesi hakkında çok daha kesin bilgiler verir. GPS alıcısı GPS uydularının konumlarını en hassas oranda bu verileri kullanarak ulaşır [18]. Efemeris her iki saatte bir güncellenir ve genellikle dört saat geçerlidir [6].

2.9 Askeri GPS Sistemi ve Yeni GPS III Uyduların Güvenlik Özellikleri

Askeri GPS alıcısı içinde M kodu şifresini çözen özel anahtar olan ve ABD Savunma Bakanlığı'nın izni ile üretilebilen özel alıcıdır. Bu GPS alıcıları askeri uygulamalarda kullanılır, aldatma ve sinyal karıştırma saldırılarına karşı dirençlidir. 2006'dan beri kullanılan GPS alıcısı yapısı ise Selective Availability Anti-Spoofing Module (SAASM) olarak bilinen ve kurcalama korumalı yapıdır. SAASM modülün içinde kırmızı anahtar saklanır ve haberleşmede kullanılacak güncel anahtarlar ve diğer güncellemeler siyah anahtarla şifrelenmiş olarak yüklenir ve içinde saklanan kırmızı anahtarla açılır.

Günümüzde anahtar yüklemenin zorluğunun artması, güvenli alanlarda kripto kleranslı personelle anahtar yükleme gibi zorluklar nedeniyle Şekil 2.8'deki Over-the-Air Distribution (OTAD) uzaktan güncelleme yapılır. Burada komuta kontrol merkezleri, anahtar merkezi ve GPS uyduları ile sahadaki GPS alıcıları uzaktan güncellenir [19].



Şekil 2.8: OTAD Yapısının Çalışması [20]

GPS aldatma saldırıları ve özellikle GPS'in askeri uygulamalarında karşılaşılan problemler nedeniyle yeni nesil GPS uyduları tasarımı şart olmuştur. Eskiyen GPS altyapısı, Rusya, Çin ve AB'nin çok daha hassas sistemlerini kurması GPS'i geriye düşürmüştür. Amerikan Hava kuvvetleri 22 yeni uydu üretimi için çağrıda bulunmuştur ve 10 adeti için üretime başlamıştır. Yeni nesil GPS uyduları 3 kat daha hassas konumlamada ve sinyal karıştırma saldırılarına 8 kat daha güçlü dayanında olacaktır. Başta yeni haberleşme protokolü ve ekstra gönderilen farklı frekanstaki sinyaller ile GPS sisteminin en yüksek hata oranı olan iyonosferik gecikme olmak üzerine pek çok soruna çözüm getirmiştir. GALILEO ile uyumlu çalışacak yeni GPS altyapısı 2023 yılına kadar 10 uydu göndererek ilk aşamanın tamamlanması planlanmaktadır.

Bölüm 3

GPS Saldırıları

3.1 GPS Saldırılarına Giriş

GPS üzerine yapılan saldırılar sistemin erişilebilirlik ve bütünlük gerekleri üzerine yapılır. Erişilebilirlik üzerine yapılan saldırıları sinyal karıştırma üzerinden, bütünlük üzerinden yapılan saldırıları da aldatma saldırıları altında incelendi. Tezin bu bölümü GPS sisteminin mevcut sorunlarının ve saldırıların anlatıldığı, literatürdeki çözümlerin gösterildiği ve bu çözümlerin tespit, önleme başlıkları altında incelendiği kısımıdır. Bu araştırmalar sonucunda tespit ve önleme çözümleri performans, uygulanabilirlik kriterlerine göre karşılaştırıldı.

3.2 Yaşanmış Saldırılar

Yaşanmış saldırıların en bilineni Amerikan Hava Kuvvetlerine ait Lockheed Martin RQ-170 İHA'sının İran tarafından 2011 yılında GPS aldatma saldırı ile Kashmar kentinde ele geçirilmesidir. Bu konuda resmi açıklama yapılmamış olmasına rağmen genel kabul önce İHA ile olan haberleşme hattı sinyal karıştırma yöntemi ile kesilir. Bundan sonra askeri P(Y) kodlu GPS hattı kesilince İHA otopilot sistemiyle merkeze dönme moduna geçmiştir. Bu aşamada İHA sivil GPS hattını kullandığından GPS aldatma devreye girmiştir. GPS aldatma saldırısı ile İran hava sahası İHA'ya ABD'nin Afganistan'daki üssü gibi gösterilmiştir ve İHA İran'a indirilmiştir. ABD daha sonra İHA'sını resmi olarak istemiş ama İran İHA'ın hava sahasını ihlal ettiğini ve geri veremeyeceklerini söylemiştir [21].

NATO Exercise Trident Juncture 2018 tatbikatı 31 ülkeden binlerce askerin katıldığı bir tatbikattır. Rusya'ya komşu Finlandiya'da 25 ekim ve 7 kasım arasında yapılmıştır. Tüm tatbikat sürecinde GPS sinyalinde kopukluklar olmuştur, bu saldırılar tatbikatta bir kazaya neden olmamış ama sivil havacılık ciddi oranda etkilenmiştir. Finlandiya hükümeti Rus büyükelçiyi dışişlerine çağırarak uyarıda bulunmuştur [22]. Rusya'nın Karadeniz kıyılarında GPS aldatma saldırıları da pek çok kez kayıt altına alınmıştır. Bu saldırıların en çok etki yapanı 2013 yılında Novorossiysk limanındaki saldırıda tüm gemilerin konumları gerçek konumlarından 30 km den fazla daha güneyde gösterdiği ve bu olayın tüm uluslararası kurumlarca bildirilip kayıt altına alındığı saldırıdır. Özellikle ticari gemi taşımacılığıyla uğraşan şirketler Rus kıyılarında bu gibi karşılaşılan pek çok durumu bildirmiştir [23]. Aynı durumla Suriye iç savaşında da ciddi oranlarda karşılaşılmaktadır ve Suriye hava sahasında GPS kullanımı kısıtlanmıştır.

Güney Kore'nin Kuzey Kore sınırında çok sayıda GPS saldırısı yapılmaktadır. Yıllardır yapılan bu saldırılar sonucu sivil havacılık ve deniz trafiği ciddi oranda etkilenmektedir. Başlıca GPS sinyal karıştırma saldırıları olmak üzere pek çok saldırı yapılması nedeniyle önlemlerin alınması şart olmuştur. Bu nedenle Güney Kore'de eLORAN sistemine geri dönüş yapılmıştır [23].

3.3 Güvenli Haberleşmenin Temelleri

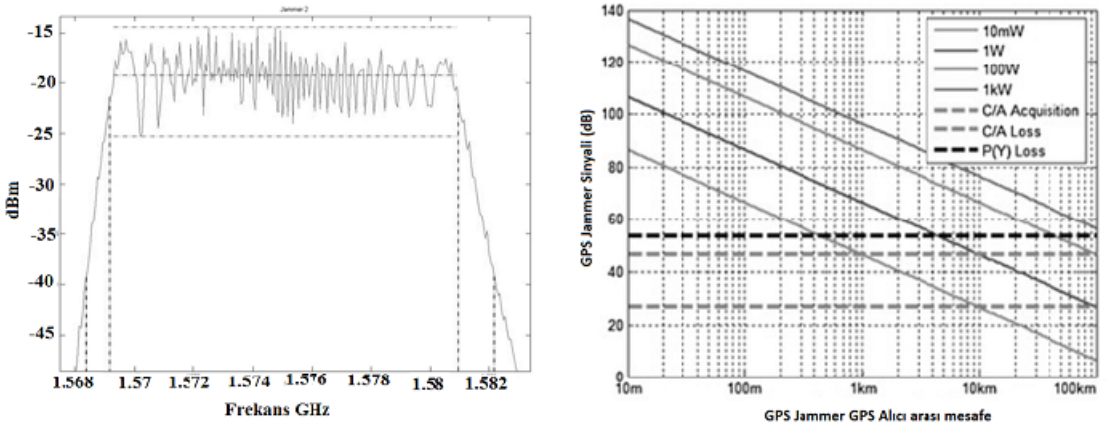
Uydu haberleşmesi yeryüzünde kablosuz olarak kesintisiz bir şekilde uydu ve anten alıcı ikilisi arasında iletişimi sağlayan haberleşmedir. Günümüzde televizyon, internet, telefon ve askeri haberleşmenin çoğu 2000 üzerinde olan bu uydular sayesinde yapılmaktadır. GPS sistemi USA Department of Homeland Security tarafından belirlenen ulusal güvenlik açısından hayati önemdeki 16 sektörün 13 tanesi ile birebir ilişki halindedir. Bu nedenle GPS sistemin güvenliği ve etkileri ulusal güvenliği etkileyecek boyuttadır.

Güvenli haberleşmenin temeli gizlilik, erişilebilirlik ve bütünlüğe dayanır. Gizlilik için gönderilen GPS mesajının şifreli bir şekilde gönderilmesi gerekmektedir. Bu kriterde sivil kullanımdaki GPS alıcıları şifresiz mesajlar alır ve bu şifresiz mesajlar saldırılara açıktır.Şifreli mesajları sadece M kodunu çözen askeri GPS alıcılarırı alır. Diğer önemli bir kriter olan erişilebilirlik üzerine yapılan saldırı yöntemi sinyal karıştırıcı ile erişimi kesmektir. Sinyal karıştırıcı ile yapılan erişim saldırılarında sinyal karıştırıcı tespit ve ona

karşı alınacak önlemler altında incelendi. Bütünlük kısmında GPS mesajında CRC kontrolü vardır ama karşılıklı doğrulama olmadığından, saldırılar bu açıklıktan yapılmaktadır.

3.4 GPS Sinyal Karıştırıcı Tespiti ve Saldırıya Dayanıklılığı

GPS sinyali çok zayıf bir sinyaldir (-160dbw) ve bu nedenle alıcı tarafından zor alınır. İyi bir sinyali almak için açık alanda olmak ve iyi bir anten-alıcı ikilisinin olması gerekmektedir. GPS sisteminin bu zayıflığından dolayı en kolay yapılan saldırı sinyal karıştırma saldırısıdır. Bu saldırıda amaç aynı frekansta kuvvetli başka sinyallerle GPS alıcısını çalışamaz hale getirmektir. GPS sinyal karıştırıcılar birkaç metreden sinyalin gücüne göre yüzlerce metreye kadar GPS sinyalini bloke edebilir.

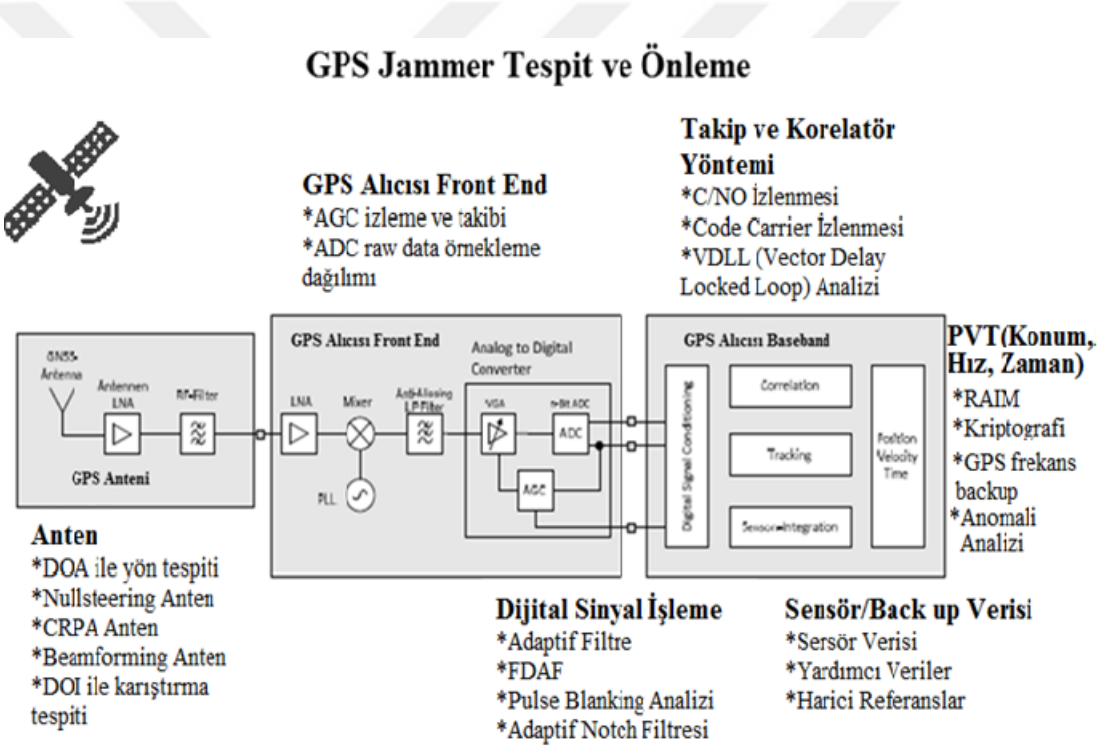


Şekil 3.1: GPS Sinyal Karıştırıcı Spektrumu ve GPS Sinyal Karıştırıcı Etkinlik Grafiği [24],[25]

Hem yaşanılan ortamdaki elektronik cihazların çalışmasından dolayı oluşan elektromanyetik sinyallerin gürültüsü hem de kötü amaçlı sinyal karıştırıcı kullanımı nedeniyle GPS alıcının bu durumlara karşı dayanıklı olması gerekir. GPS sinyal karıştırıcı tespiti çoğu GPS alıcısı üreticinin sağladığı standart bir özelliktir.

GPS sinyal karıştırıcı tespiti; GPS anteni, GPS alıcısı front-end ve GPS alıcısı baseband olarak Şekil 3.2'deki gibi 3'e ayrılan kısımlarında yapılır. Bunları da tespit, önleme ve her ikisinin olduğu yöntemler olarak ayrı ele alınabilir. Anten kısmında saldırı çeşitine

uygun anti-jammer anten kullanımı en önemli kriterdir. GPS alıcısı front end kısmında ise saldırı tespiti sinyal analizi ve başlıca filtreler kullanılarak yapılır. Bunlarla hem GPS sinyal karıştırma tespiti hem de saldırıya karşı önleme yapıla bilinir. Sinyal kısmında AGC ve ADC örnekleme-dağılım analizi üzerinden analizler yapılır. Filtre kısmında adaptive digital filtering teknolojisi, çoklu SAW (Surface Acoustic Wave) filtre kullanımı başlıca yöntemlerdir. Tespit yönteminde GPS sinyalinin yüksek çözünürlükle dijitalleştirilmesi ve bu sinyallerin analizi yapılması vardır. Sinyal işlemleri sırasında low pass, high pass, band pass filtreler kullanılarak temizleme işlemleri yapılır ve bu aşamalarla normalden güçlü olan GPS sinyalinin tespiti yapılır [26].



Şekil 3.2: GPS Jammer Tespit ve Önleme Yöntemleri

GPS sinyal karıştırıcıya dayanıklı anten kullanımı sinyal karıştırma saldırılarında ilk alınacak önlemdir. GPS anten kısmında FRPA, Horizon Nuller, Selective Nuller, Beamformer, Adaptive CRPA, STAP/SFAP All in view Adaptive CRPA ve Vector tracking adaptive CRPA en bilindik sinyal karıştırıcıya dayanımlı anten türleridir [27]. Tüm bu antenlerin maliyet, kullanım alanı, boyut ve performans gibi özelliklerine göre farklı kullanım alanları vardır. Aktif anti jammer GPS antenler çözümlerinde ise öncelikle sinyal

karıştırıcı sayısı ve konumları bulunur sonra yönlü antenlerle sinyal karıştırıcı kaynaklarının olduğu yerlere aynı frekansla sinyaller basılıp bu yöndeki karıştırıcı sinyaller bastırılır. Sinyal karıştırıcı kaynakların sayısı kaçsa tüm kaynakların bu şekilde söndürülmesi gerekir. Bu yöntem aktif anti-jammer GPS sistemi olarak adlandırılır. GPS alıcısı çıktısının kontrolü, yardımcı sensör kullanımı, RAIM (Receiver Autonomous Integrity Monitoring - Alıcının Bağımsız Doğruluk Kontrolü Yöntemi) ile de GPS sisteminin kontrolü yapılmaktadır.

3.5 GPS Aldatma Saldırısı

GPS aldatma saldırısında gerçek GPS sinyalinden daha güçlü sahte GPS sinyalleri oluşturulur. Bu durumda GPS alıcısı sahte sinyali seçecektir. Sahte sinyali sinyal jeneratörü, USRP ya da GNSS uydu simülatörü gibi cihazlar kullanılarak oluşturulabilir ve aldatma saldırısı hedefi istenilen zaman ve konum bilgisini gerçek gibi alır. GPS aldatma saldırısının uygulamaları arasında en basit olanı balıkçılar ve gemiler tarafından Automatic Identification System (AIS) üzerinden devlet kurumlarınca takiplerini engellenmesi örneği alınabilinir. Burada yasak olan bölgelerde avlanma, atık boşaltma gibi kanunsuz işlerde kullanılır. Birkaç bin dolarlık basit GPS kitleriyle aldatma sağlanabilir ama daha kompleks saldırılar Şekil 3.3 'deki gibi yüksek bütçeli GPS sinyal jeneratörü, GNSS simülatörler gibi araçlarla yapılabilmektedir. Bu tez çalışmasında da bunları tek tek anlatarak aldatma tespit ve önlemlerinden bahsedilmektedir. Saldırı tespitleri ve önlemleri anten bazlı ve alıcı bazlı olarak ayrı ayrı anlatılmaktadır. GNSS simülatörleri GPS tabanlı ürünlerin testi için yapılmıştır, asil amaçları üretilen GPS alıcısı performans testleridir. Burada GPS parametrelerini (Date/Time,Clock Parameters, Satellite ID PRN code, Ephemeris, Almanac) istenilen şekilde ayarlayıp saldırı sinyalleri GPS aldatma saldırısı hedefine yönlendirilir.

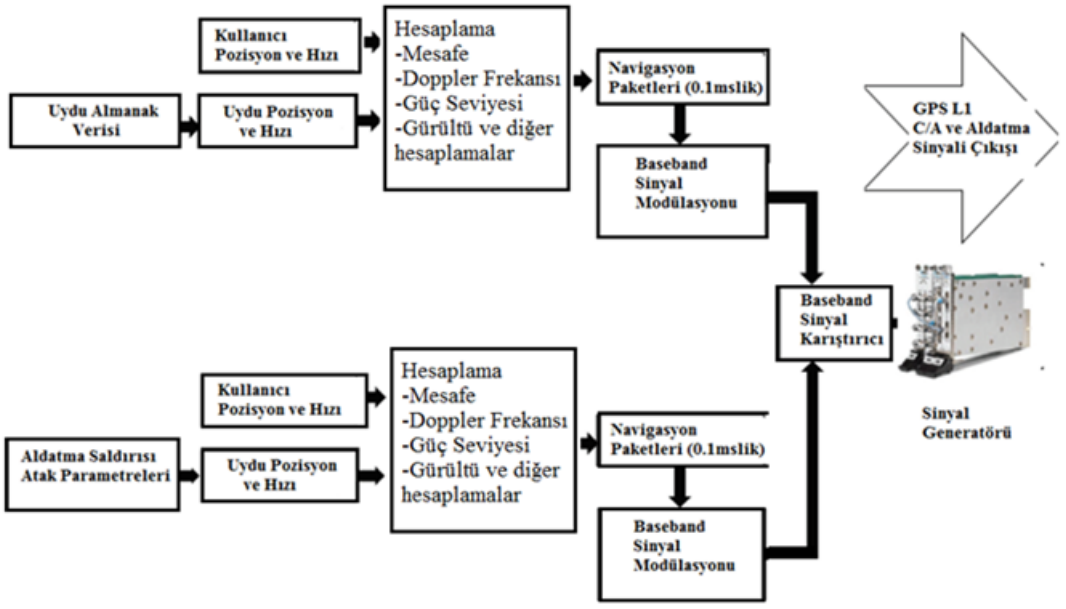
Şekil 3.3: GNSS Simülatör Örnekleri [28]

GPS aldatma senaryoları Şekil 3.4 'deki gibi farklı başlıklar altında ele alınabilir. Basit saldırı senaryosunda GNSS simülatörler tek başına kullanılır. Bu aldatma saldırılarında aldatma saldırısı hedefi ile GPS alıcısı arasında sinyal güç seviyesi, faz, doppler etkisi ve veri içeriği gibi başlıklarda senkronizasyon yapılmamaktadır. Tek kaynaktan sinyal üretilip saldırı yapılmaktadır ve tespiti kolaydır.

Orta ölçekli saldırılarda daha kompleks saldırılar yapılır; burada saldırgan hedefe daha yakın ve hedefin gerçek hız, zaman ve konum bilgisini bilip ona göre senaryolar gerçekleştirebilir. GPS aldatma saldırganı daha portatiftir ve hızlı bir şekilde yeni konumdan saldırılar gerçekleştirebilir. Basit saldırılarda kullanılan GNSS simülatörler ticari ürünler olduklarından piyasada rahatlıkla bulunabilmekteyken portatif ürünler için özel çözümler üretilmesi gerekmektedir. Bu saldırı senaryosunda doppler etkisi, güç seviyesi, faz farkı ve veri içeriği gibi veriler hedef ile senkronize edilebildiği için bu tip saldırılarda temel tespit yöntemi olarak DOA kullanılabilir. Burada da tek kaynak üzerinden saldırı olduğundan DOA ile saldırı tespiti kolaydır.

Şekil 3.4: GPS Saldırma Senaryoları [29]

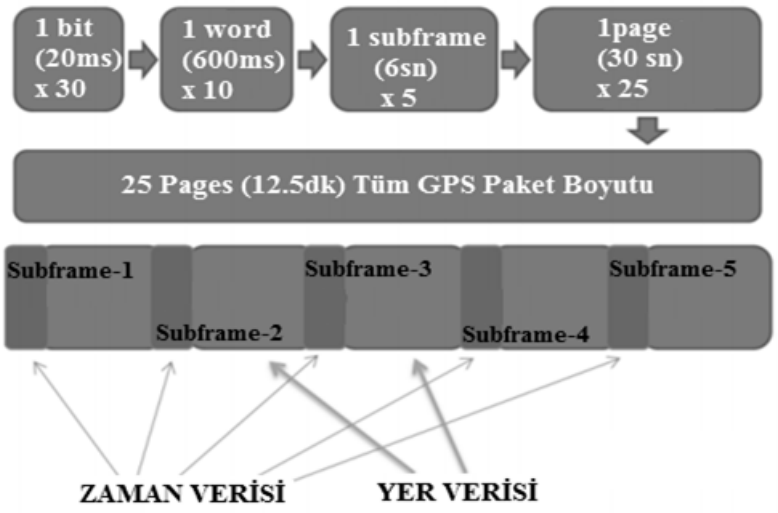
Gelişmiş ve orta ölçekli saldırılarda Şekil 3.5 'deki gibi GPS aldatma saldırısı kurbanı ile senkronizasyon işlemi vardır. Gelişmiş saldırılarda saldırgan hem hedef GPS alıcısı ile verilerini senkronize eder hem de koordine edilmiş çoklu GPS aldatma saldırı kaynakları ile DOA GPS aldatma tespitine karşı önlem almış olur. Bu saldırı ile tekli kaynaktan yapılan ve kolayca uygulanabilen senaryodan çoklu ve birbiri ile koordineli kompleks bir saldırı yöntemine geçilmiştir. Bu da gelişmiş saldırı senaryosunun uygulanabilirliğini zorlamaktadır [29].



Şekil 3.5: GPS Orta ve İleri Seviye Aldatma Saldırısı [30]

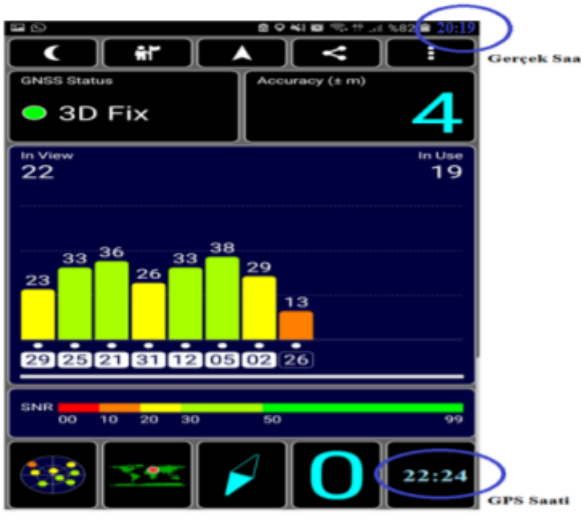
Bu aşamada saldırılar kesintisiz ve kesintili olarak yapılır. Kesintisiz saldırıda önce hedef GPS alıcısına gerçek sinyallerden düşük değerlerde yayın yapılmaktadır ve sonra bu sahte GPS sinyalleri daha da kuvvetlendirilerek gerçek konumlamadan sahte konumlamaya çok yumuşak geçiş yapılır ve GPS aldatma saldırısı tespit yöntemlerinden çoğunu etkisiz hale getirir. Kesintili saldırılarda ise çok daha keskin geçişler vardır ve konum, sinyal kuvvetleri ve diğer parametrelerdeki ani değişimler nedeniyle saldırı tespit daha başarılıdır [31].

GPS aldatma saldırısı fiziksel katmanda yapılan bir saldırı türüdür. Bu saldırılarda amaç hedef GPS alıcısını yanlış konum belirlemeye zorlamaktır. GPS aldatma saldırısında Şekil 3.6 'da gösterildiği gibi navigasyon mesajının içeriğini değiştirerek ya da navigasyon mesajının varış süresini değiştirerek yapılmaktadır. Gerçek zamanlı saldırılarda navigasyon mesajı anlık değiştirilebilir ya da gelen GPS sinyali geciktirilerek aynen hedef GPS alıcısına gönderile bilinir.



Şekil 3.6: GPS Paket Yapısı, Zaman ve Yer Verisi

GPS aldatma saldırıları içinde en kolay yapılan saldırı çeşidi kayıt ve tekrardan oynatma saldırısıdır. Atomik saat verisini elde etmek için GPS sistemi kullanan sistemler bu saldırının öncelikli hedefleridir. USRP ile alınan kayıtlar tekrardan oynatılarak GPS alıcısı manipüle edilir. Şekil 3.7 'de gösterildiği gibi saat verisi bu saldırıyla değiştirilebilinir.



Şekil 3.7: Temsili GPS Kayıt ve Tekrardan Oynatma Saldırısı

Başta bankacılık, finans, savunma gibi sektörlerde saat hesabı % 99 üzerinde NTP (Network Time Protocol) ile yapılmaktadır. Burada UTC atomik saat verisi de GPS üzerinden alınabilmektedir. GPS üzerinden yapılacak saldırılarda tüm bu sektörler etkilenecektir.

Bu nedenle özellikle network firmaları ve data merkezleri GPS time anomalilerini tespit eden Şekil 3.8 'deki gibi firewall ve güvenlik analizi yazılımları geliştirilmiştir.

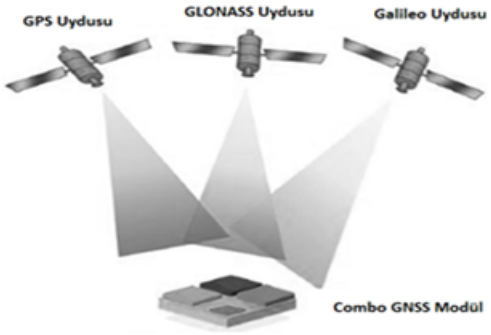
Şekil 3.8: GPS Firewall Kullanım Senaryosu [32]

3.6 Çoklu Sensör Çözümleri

Bu tez kapsamında bahsedeceğimiz GPS aldatma saldırıları önlemlerden biri de çoklu sensör kullanımıdır. Amaç farklı sensör kullanımı yaparak aldatma saldırısı gerçekleştiğinde aldatma saldırısı tespiti yapılması ve konumunu doğrulamasıdır. INS, çoklu GNSS kullanımı, RTK, Radar altimetre gibi sensör kullanımı ile GPS saldırı tespiti kolayca yapılabilmektedir.

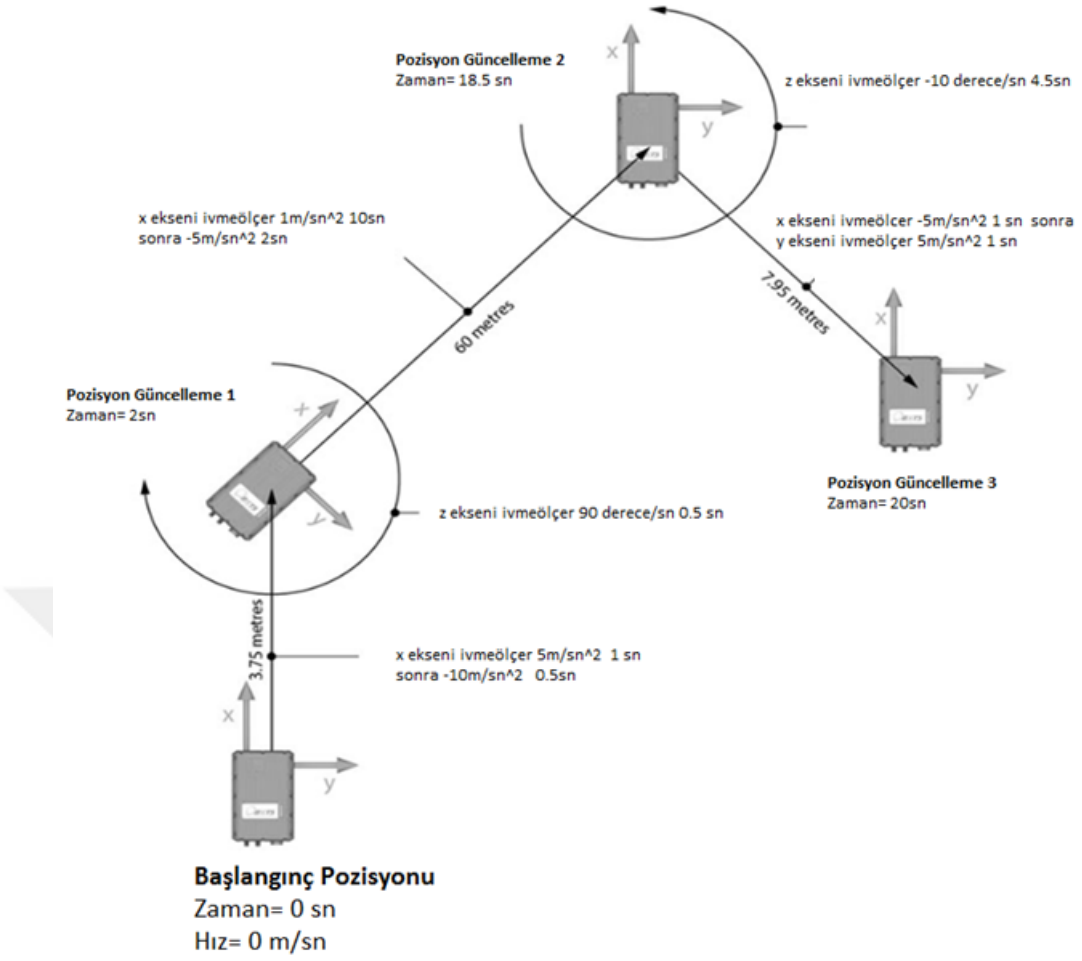
Çoklu modüller içinde birden fazla GNSS sisteminin desteği olan GNSS alıcılarıdır. En popüler olanı GPS/GLONASS çoklu modülüdür. Tüm GNSS sistemlerinden konum bilgisinin alınması ve kontrol edilmesi ile aldatma saldırılarına karşı koruma elde edilir.

Saldırgan tüm GNSS sinyallerine bloke etmesi ve aldatma saldırısı yapması gerekmektedir. Bu nedenle çoklu modul kullanımı hem daha hassas konum bilgisini alınmasını sağlar hem de saldırı tespitinde kullanılır.



Şekil 3.9: Çoklu GNSS Alıcısı

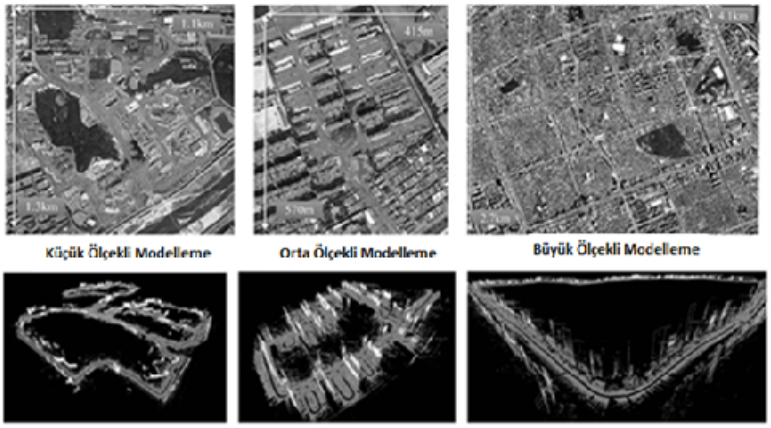
INS sistemleri hareket sensörleri, ivme sensörleri, jiroskop ve magnetometreler kullanılarak aracın hareketindeki, ivmesindeki, açısındaki ve manyetik alandaki değişimlerden elde delilen verilerin konumlamada kullanılması üzerine çalışmaktadır. Özellikle yüksek hızlı araçlarda (Uçak, füze, v.b.) ve GPS sinyalinin çekmediği yerlerde (denizaltı, v.b.) konumlama için kullanılmaktadır [33]. GPS ile birlikte kullanılan ve askeri uygulamalarda en yaygın yardımcı sensör verisidir. Magnetometre dünyanın manyetik alanından yararlanıp bu alandaki en küçük değişimi bile sezip bunu konumlama tespitinde kullanılacak veri olarak sağlarlar. Barometreler hava basıncını ölçen sensörlerdir. Yüksekliğe bağlı olarak hava basıncı değişmektedir. INS sistemlerinde barometreler bir data girdisi olarak kullanılmaktadır. Hava durumu değişimlerinden basınç farklılıkları oluşur, sensör verisi kullanımında bunun da dikkate alınması gerekmektedir.



Şekil 3.10: GPS/INS Örnek Çalışması [33]

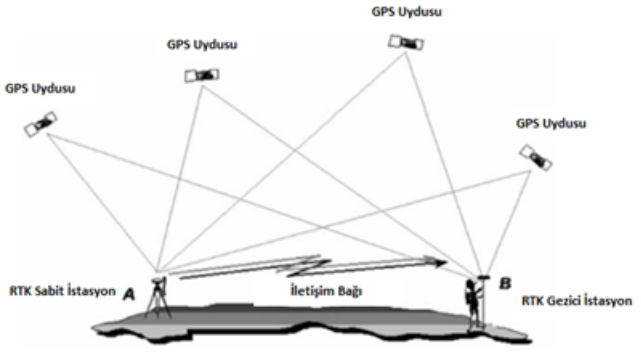
Radar altimetre daha çok hava araçlarında kullanılan ve yükseklik verisinin hesaplanmasına yarayan araçtır. Hava aracından belli periyotlarda aşağıya RF sinyalleri basılır ve bunların geliş zamanından yükseklik hesaplanır, çalışma mantığı radarlarla aynıdır. Bu sistemin geliştirilmesiyle hava araçları için radar altimetre ve barometrik altimetrenin sayısal arazi verisiyle karşılaştırılarak geliştirilen GPS'siz konumlama sistemleri de yapılmıştır [34]. SLAM (Simultaneous localization and mapping- Eş zamanlı konum belirleme ve haritalama) yöntemi özellikle otonom araçların hayatımıza girmesiyle onların görevlerini yapabilmeleri için çevrelerini haritalamaları ve konumlarını bilmeleri gereğiyle ortaya çıkmıştır. Bunu yaparken üzerinde taşıdıkları çok sayıda sensörlerden yararlanırlar ve yaklaşık çözüm yöntemleri parçacık filtresi, genişletilmiş Kalman filtresi (EKF) ve GraphSLAM algoritmaları kullanarak haritalama yaparlar. Lokal bazlı haritalama ve

geçmişe doğru sorgulama yaparak küçük ölçekli konumlama çözümü olarak kullanılabilinir [35]. SLAM genellikle küçük bölgelerde haritalamada kullanılsa da veriyi kullanabilme ve işleme yeteneğine göre daha büyük boyutlu uygulamalarda da kullanılabilir.



Şekil 3.11: SLAM Örnek Haritalama [36]

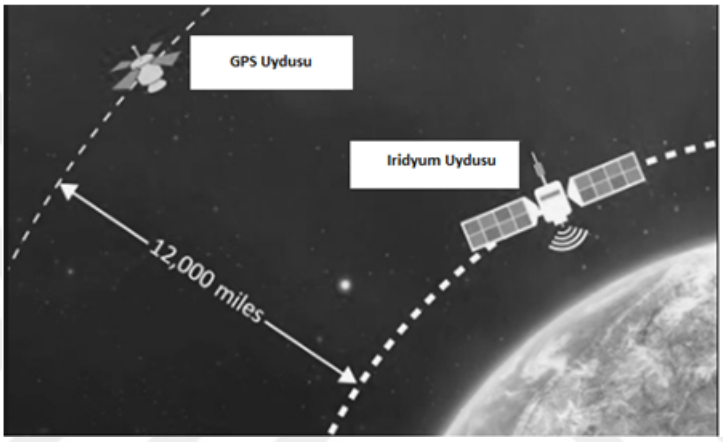
RTK: GPS sistemine yapay olarak eklenen bozulmaların, uydu saati, iyonosferik gecikmeler gibi kaynaklı hataları bir referans istasyonundan sürekli ölçülüp telsiz üzerinden gezici istasyona düzeltme olarak gönderilmesi üzerine kurulu GPS ölçüm metodudur. Yatayda ortalama iki santimetre düşeyde dört santimetreye kadar doğruluk sağlar. Uygulamada RTK sistemleri tek bir baz istasyonu alıcısı ve mobil birimlerin bir dizisini kullanır. Çoğu ülkede belirli frekanslar RTK amacıyla özel olarak tahsis edilmiştir.



Şekil 3.12: RTK Çalışma Sistemi [37]

STL: Dünya çevresindeki 66 adet Iridyum uydularını kullanarak konum ve zaman belirleme sistemidir. GPS sinyalinden bin kat daha kuvvetlidir, bu nedenle kapalı alanlarda

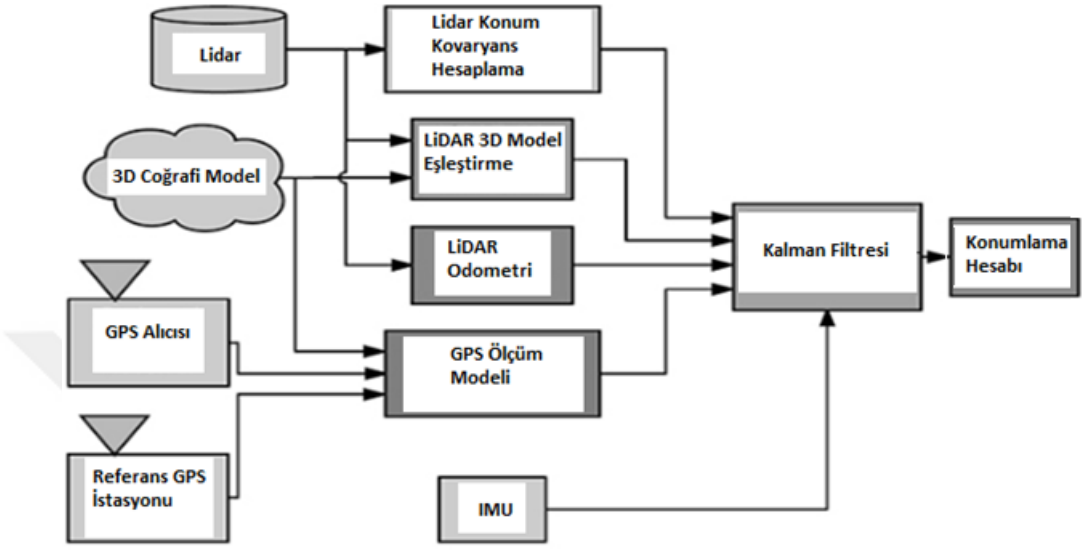
(belli sınırlar içinde) da konum belirlemede kullanılabilir. 2016 yılından itibaren aktif olarak kullanılmaktadır. GPS den farklı olarak sivil kullanım için şifreli versiyonu da vardır. GPS uydularına göre çok daha yakın ve çok daha kuvvetli sinyal gönderdiklerinden dolayı sinyal karıştırma saldırılarına dayanıklıdır. GPS gibi küresel ölçekte çalışabilmektedir. GPS'e göre dezavantajı konum ve zaman hassasiyetinin düşük olmasıdır; ama deniz araçları gibi sivil GPS saldırılarının çokça karşılaşıldığı alanlarda bu sorunları çözdüğü için aktif olarak kullanılmaktadır [38].



Şekil 3.13: STL Iridyum Uydusu[38]

Sensör füzyonu: Çoklu sensör kullanımında birçok sensör verisini kullanıp anlamlı hale getirilmesidir. Günümüzde aynı amaçta kullanılan pek çok sensör vardır, bunun dışında tek sensörden elde edilen veriler de yeterli hassasiyette değildir. Bu nedenle pek çok sensör verisi uygun algoritmalar ve filtreler kullanılarak en uygun verinin elde edilmesi gerekir. Sensör füzyonu konumlama, robotik, otomasyon, tıp ve endüstriyel uygulamalarda çokça kullanılmaktadır. Sensör füzyonunda en çok kullanılan algoritmalar central limit theorem (CLT), kalman filter, bayesian network, dempster - shafer theory, convolutional neural network'dür. Bunlar arasında en popüleri ve en çok GPS uygulamalarında kullanılanı ise kalman filtresidir. Kalman filtresi dinamik sistemlerin durum uzay modeliyle gösterilip önceki verilerini ve giriş-çıkış bilgilerini kullanarak sistemin durumunun tahmin edilmesidir. Kalman filtresi, geleneksel tahmin edicilerde olduğu gibi filtreleme özelliğine rağmen, sistemin ölçülemeyen durumlarını tahmin etmek için de çok güçlü ve yeteneklidir [39]. Şekil 3.14'de GPS sisteminin kalman filtreli çoklu sensör kullanımı örneğiyle GPS veri doğrulaması yapılmaktadır. Sensör füzyonu sayesinde çoklu sensör

kullanımı ve GPS doğrulaması yapılabilmektedir. Bu da GPS aldatma saldırısı tespitini sağlamaktadır.

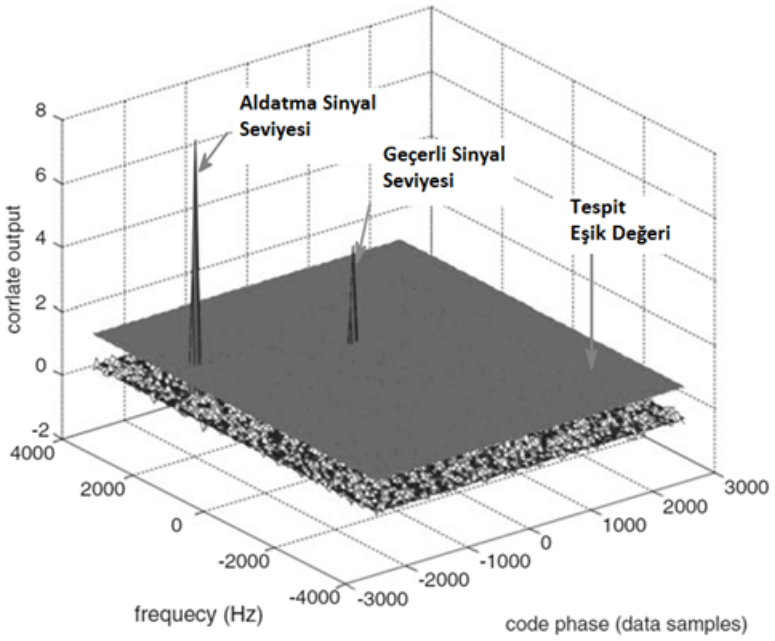


Şekil 3.14: Sensör Füzyonu GPS Örneği [40]

3.7 GPS Alıcı - Anten Tabanlı Çözümler

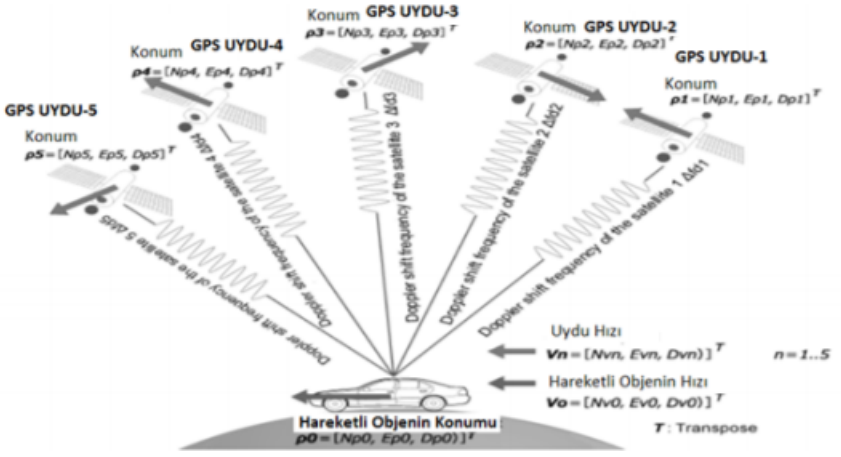
Tezin bu kısmında GPS saldırılarının tespiti ve saldırıya dayanım konusunda en başarılı sonuçların alındığı yer olan GPS alıcısı ve anten kısmı anlatılmıştır.

GPS sinyalinin gücünün ortalaması bellidir. Çevresel etkenler, hava ve atmosferik olaylar sinyal seviyesini etkileyebilir ama aldatma sinyalleri Şekil 3.15'deki gibi gerçek sinyallerden en az 2 db, 3 db fazla olması gerekmektedir. Adaptif maksimum sinyal seviyesi filtresi kullanılarak aldatma sinyalleri temizlenebilir. GPS sinyallerinin güçleri kayıt altına alınır ve ani değişimler bulunur. Bu değişimler kullanıcıya alarm olarak bildirilir. Sinyal kuvvetindeki değişim zaman içinde gerçekleşmesi lazımdır, GPS sinyali hep aynı güçte ve kusursuz geliyorsa bu durumda anomali olarak tespit edilip kullanıcıya bildirilmesi gerekmektedir. Pr^2 sinyal gücünün değişim oranının takibi ve bağıl gücün izlenmesi de aldatma tespitinde kullanılır [41].



Şekil 3.15: GPS Sinyal Seviyesi Aldatma Saldırısı analizi [42]

Doppler efekti ve analizi GPS aldatma saldırı tespitinde kullanılan başlıca yöntemlerden biridir.Doppler etkisi, bir RF dalga kaynağı ile gözlemcinin birbirlerine göre hızla hareket etmeleri durumunda çıkan dalga boyu değişmesidir. Gözlemci ve kaynak arasındaki değişikliklerin frekans değişime neden olması ve bunun matematiksel olarak yorumlanmasıdır. GPS alıcıları konum çözümüne ve uydu konumuna sahiptir. GPS alıcısının, her bir GPS uydusuna göre göreceli hızı bu şekilde elde edilebilir.



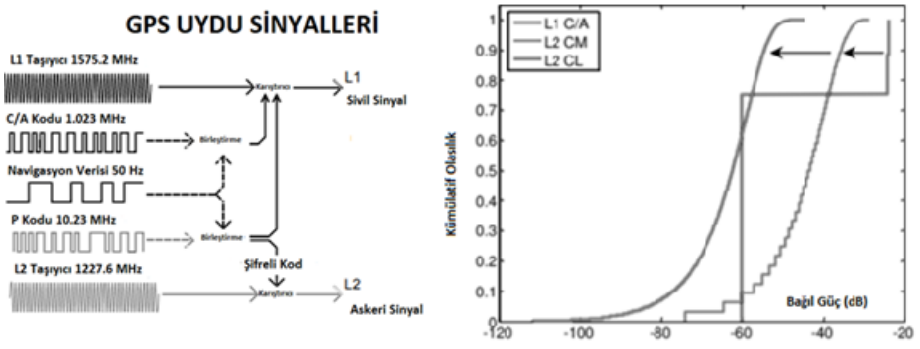
Şekil 3.16: Doppler Kayması Kontrolü [43]

Doppler kayması taşıyıcı frekansını değiştirdiğinden, tek bir verici kullanarak yapılan saldırılarda saldırı kaynağı tarafından tüm uyduların hareketinin taklit edilmesi çok zor olacağından aldatma saldırısı tespit edile bilinir. Orta ve ileri seviye saldırı da L1 frekansında uyduların hareketi ve GPS saldırgan hedefin hareketinden Doppler frekansı gecikmesi aynı olacak şekilde yayın yaparak saldırı gizlenir. Tablo 3.1'de L1 frekansı üzerinden yapılan örnek bir çalışmaya ait fark hesaplama ve saldırı tespiti gösterilmiştir.

Tablo 3.1: Örnek GPS Doppler Frekans Gecikmesi Hesaplama Tablosu [18]

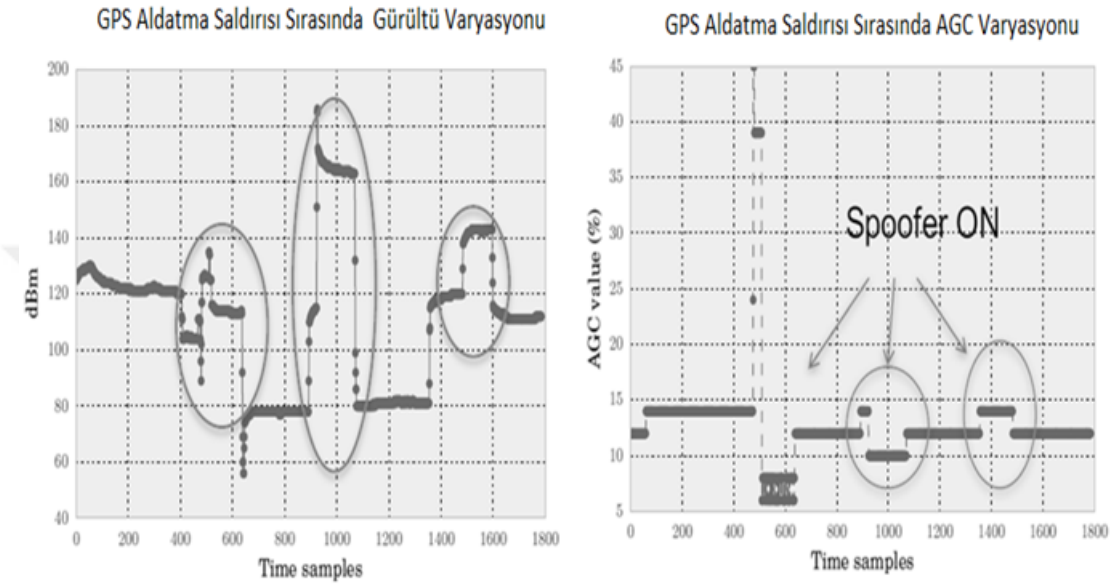
GPS ID	Doppler [Almanak] Hz	Doppler [Hesaplanan] Hz	Fark Hz
3	1955.626	1903.088	-52.538
6	-3641.199	-3687.801	-46.602
9	2888.578	2831.867	-56.711
15	1968.829	1921.299	-47.530
18	293.783	245.853	-47.929
21	-522.125	-573.658	-51.533
22	1740.733	1693.657	-47.076
26	-2986.664	-2986.664	-50.947

Tüm GPS uyduları GPS sinyali 1575.2MHz L1 taşıyıcı frekansı ve 1227.6 MHz L2 taşıyıcı frekansı ile taşınır. P kodu 10.23 Mhz de 266 günde bir kendini tekrar eden GPS uydularının haftalık PRN ID'lerini yaydıkları frekanstır. P kodu haftada bir değiştiğinden çarpraz korelasyon sonucu anlık değişmez. L1 L2 çarpraz korelasyona bakarak bu iki sinyal arasındaki korelasyon sonucunun farklılığından GPS aldatma saldırısı tespiti yapıla bilinir.



Şekil 3.17: L1 ve L2'nin Çapraz Korelasyonu [44]

GPS sinyalinin gürültü seviyesin izlenmesi, sinyal kalitesi izleme yöntemi (Signal Quality Monitoring SQM), CNR (Carrier Noise Ratio) seviyesinin izlenmesi, AGC (Automatic Gain Control) seviyeleri, sinyal gürültü seviyesi ve APD (Autocorrelation Peak Distortion) kontrolü aldatma saldırısı tespitinde kullanılır [42].



Şekil 3.18: GPS Gürültü ve AGC Aldatma Saldırısı Etkisi [42]

GPS alıcıları daha önceden GPS uydularının efemeris verilerine sahiptir ve aldatma saldırısı olduğunda efemeris verileri de değişir. Alınan ve önceden indirilmiş olan verilerin karşılaştırılmasıyla ortaya çıkan farklılık aldatma saldırısı tespiti için kullanılır. Uydu almanak ve efemeris verileri GPS uydularının izleyecekleri rotaları belirten verilerdir. Her bir uydu tarafından ve 30 saniye aralıklarla yayınlanan efemeris veriler kullanılarak GPS uydu konumları çok hassas şekilde hesaplanabilir. GPS uydu konumlarını bulmak için Tablo 3.2'deki uydu efemeris parametreleri GPS alıcısı ile elde edilip işlenmesi gerekir.

Tablo 3.2: Uydu Efemeris Veri Parametreleri

M_o	Referans anında ortalama anomali
Δn	Hesaplanan değerden ortalama hareket farkı
E	Eksentrisite
$\sqrt{a}$	Büyük yarı eksenin karekökü
Ω_o	Referans anındaki rektasansiyon
Ω	Yer yakını noktası (Perigee) argümanı
C_{uc}	Enlem argümanına kosinüs harmonik düzeltme miktarı (Rad)
C_{us}	Enlem argümanına sinüs harmonik düzeltme miktarı (Rad)
C_{rc}	Yörünge yarıçapına kosinüs harmonik düzeltme miktarı (m)
C_{rs}	Yörünge yarıçapına sinüs harmonik düzeltme miktarı (m)
C_{ic}	Eğim açısına kosinüs harmonik düzeltme miktarı (Rad)
C_{is}	Eğim açısına sinus harmonik düzeltme miktarı (Rad)
T_{oe}	Efemeris referans zamanı (s)
İOD	Veri zamanı (Efemeris için)

Burada efemeris verileri alındıktan sonra GPS uydu konum bilgisini hesaplamak için ECEF koordinat sistemi kullanılır. Elde edilen parametreler Tablo 3.3'deki ECEF denklemlerinde yerine konularak hesaplama yapılır.

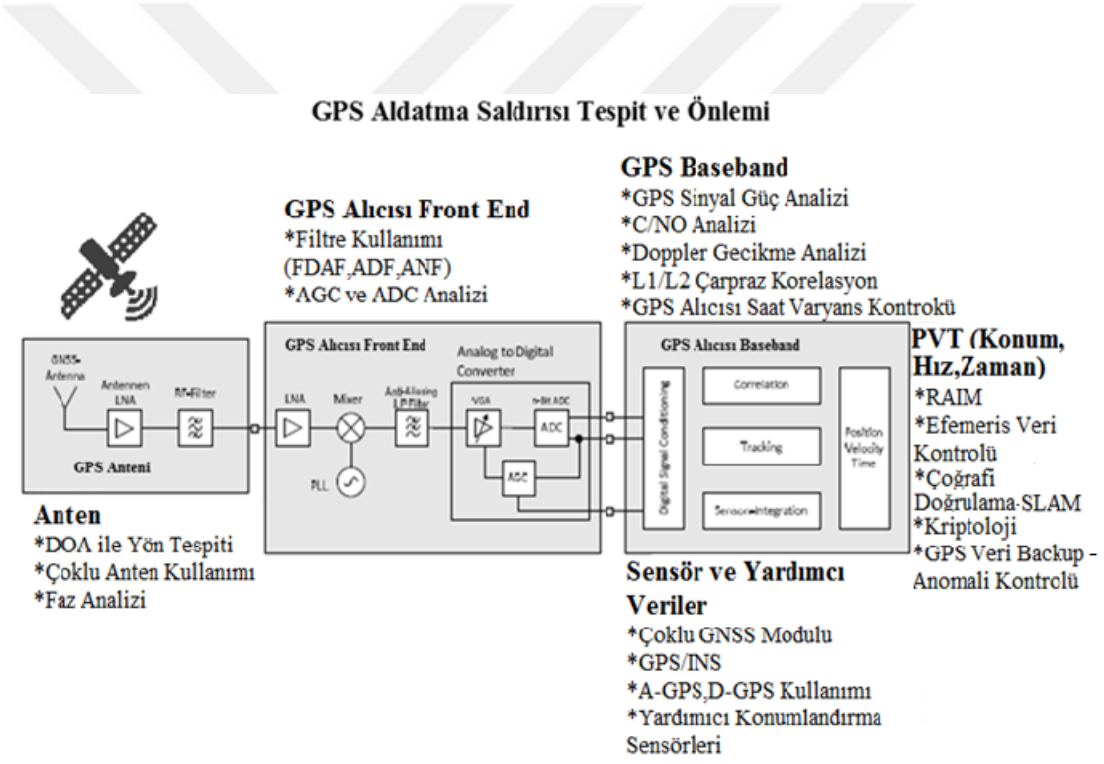
Tablo 3.3: ECEF Denklemleri

GM=3.986005 x 10^{14} m^3/S^2	WGS 84 sabiti, yerküre evrensel yerçekimi Parametre
W_e=7.292115 x 10^{-5} rad/s	WGS 84 yerküre rotasyon oranı
$\Pi = 3.1415926535898$	Pi değeri
T=$2\Pi/\sqrt{GM/A^3}$	Uydu orbital periyot
n_0= $\sqrt{GM/A^3}$	Hesaplanan ortalama hareket
n=n_0 +Δn	Doğrulanan ortalama hareket
$\overline{M_k}$=$\overline{M_0}$+nt_k	Ortalama anomeli değeri
E_k=M_k+esin E_k	Eccentric anomeli keppler denklemi
Φ_k=V_k+Ψ	Enlem argümanı
$\delta u_k = C_{rc}\cos 2\phi_k + C_{us}\sin 2\phi_k$	Enlem argümanı düzeltmesi
$\delta r_k = C_{rc}\cos 2\phi_k + C_{rs}\sin 2\phi_k$	Yarıçap düzeltmesi
$\delta i_k = C_{ic}\cos 2\phi_k + C_{is}\sin 2\phi_k$	Eğim düzeltmesi
$u_k = \phi_k + \delta u_k$	Doğrulanmış enlem argümanı
$r_k = A(1 - e\cos E_k) + \gamma r_k$	Doğrulanmış yarıçap
$i_k + i_0 + it_k + \delta i_k$	Doğrulanmış eğim
$\overline{X_k} = r_k \cos u_k$	Orbital düzlemde x konumu
$\overline{Y_k} = r_k \sin u_k$	Orbital düzlemde y konumu
$\Omega_k = \Omega_0 + (\Omega - \omega_e)t_k - \omega_e t_{0e}$	Düzeltilmiş boylam düğümü
$X_k = \overline{X_k}\cos\Omega_k + \overline{Y_k}\sin\Omega_k \cos_{i_k}$	Düzeltilmiş geosentrik uydu x koordinatı
$Y_k = \overline{X_k}\sin\Omega_k + \overline{Y_k}\cos\Omega_k \cos_{i_k}$	Düzeltilmiş geosentrik uydu y koordinatı
Z_k=$\overline{Y_k}\sin i_k$	Düzeltilmiş geosentrik uydu z koordinatı

Günlük efemeris bilgilerini https://cddis.nasa.gov adresinden indirilebilinir. Bu veriler üzerinden uyduların konumlarına ulaşılmaktadır. ECEF denklemiyle hesapladığımız verileri indirdiğimiz günlük verileri karşılaştırarak saldırı tespitini yapılmaktadır.

GPS alıcısının içinde kullanılan kristal ya da osilatörün kalitesine göre normal çalışmada ortalama saat biası ile hareket eder. Aldatma saldırısı olduğunda saat biası ani değişimler gösterecektir. Bunun nedeni, tüm sahtecilik sinyallerinin aldatma saldırganı ile alıcı arasında ortak bir gecikme yaşanmasıdır. Bu durumda bilinen bir GPS aldatma saldırı tespit yöntemidir.

GPS saldırı tespiti ve önlemi Şekil 3.19'deki gibi GPS anten, GPS alıcısı front-end ve GPS alıcısı baseband olarak 3'e ayrılabilir. Bunları da tespit, önleme ve her ikisinin olduğu yöntemler olarak ele alınabilir. Anten kısmında çoklu anten kullanımı, DOA ve faz analizleri, Front-end de filtreler, ADC, AGC analizleri, Baseband ve veri çıkışında ise sinyal analizleri, veri karşılaştırmalar ve sensör kullanımları vardır.



Şekil 3.19: GPS Aldatma Saldırısı Tespit ve Önlemi

Yasal engel ve önlem olarak Türkiye'de GPS aldatma ve sinyal karıştırma uygulamaları haberleşme hürriyetini engellediğinden TCK'da "Elektronik haberleşme kanununa aykırı hareket etme " eylemi nedeniyle yasal yaptırımları vardır. BTK'da sinyal karıştırıcıların, 5809 sayılı elektronik haberleşme kanununun 2. maddesi 3. fıkrasında belirtilen kurumların dışında kurulması, kullanılması, üretimi ve ithalatı yasaklanmıştır.

Tüm bu yapılan araştırma ve metotları özetlemek istersek sadece askeri GPS alıcısı kullanmak pek çok sorunu çözebilir ama kompleks saldırılarda yetersiz kalmaktadır. Bu durumda sensör bazlı ve alıcı-anten bazlı çözümlerle önlem almak gerekir. GPS/INS sistemlerinin kullanımı, çoklu GNSS modülü, radar altimetre, büyük boyutlu SLAM uygulamaları, coğrafi doğrulama gibi ek sensörlerin kullanımı GPS sisteminin aldatma tespiti ve gerçek konum verisinin bulmasında yardımcı olur. A-GPS ve D-GPS uzun zamandır kullanılan ve hemen hemen tüm GPS alıcılarda mevcut olan bir özelliktir. Bu özellikler sayesinde de referans GPS istasyonları ve GSM üzerinden de konum doğrulama ve saldırı tespiti yapıla bilinir. Havacılık ve denizcilik uygulamalarında ELORAN ve STL tek başlarına GPS aldatma saldırılarına dayanımı sağlamaktadırlar. GPS Alıcı-Anten tarafında GPS sinyal analizi, frekans analizin, efemeristik data analizi yöntemleriyle de yüksek başarımda GPS saldırı tespiti yapıla bilinmektedir. Tablo 3.4'de tez kapsamında bahsettiğimiz yöntemlerin uygulanabilirlik-performans karşılaştırması verilmiştir.

Tablo 3.4: Yöntem - Performans Tablosu [45]

Yontem	Saldırı Tipi	Uygulanabilirlik	Performans
Çoklu GNSS Modül	Aldatma Saldırısı	Orta	Orta
GPS/INS	Aldatma Saldırısı	Orta	İyi
SLAM - Çoğrafi Doğrulama	Aldatma Saldırısı	Zor	İyi
A-GDS/D-GPS	Aldatma Saldırısı	Kolay	Kötü
CRPA Anten	Aldatma Saldırısı, Sinyal Karıştırma Saldırısı	Orta	Orta
Aktif Anti Jammer GPS	Sinyal Karıştırma Saldırısı	Zor	İyi
GPS Sinyal Gücünün İzlenmesi	Aldatma Saldırısı, Sinyal Karıştırma Saldırısı	Orta	İyi
Doppler Kayması Kontrolü	Aldatma Saldırısı	Orta	Orta
L1 ve L2'nin Çapraz Korelasyonu	Aldatma Saldırısı	Orta	Orta
Efemeris Verilerini Kontrolü	Aldatma Saldırısı	Kolay	Orta
DOA	Aldatma Saldırısı, Sinyal Karıştırma Saldırısı	Orta	İyi
Faz Farkı Analizi	Aldatma Saldırısı	Zor	Orta
GPS Sinyal Analizi	Aldatma Saldırısı, Sinyal Karıştırma Saldırısı	Orta	İyi
GPS Alıcısı Saat Varyans Kontrolü	Aldatma Saldırısı	Orta	Orta

Bölüm 4

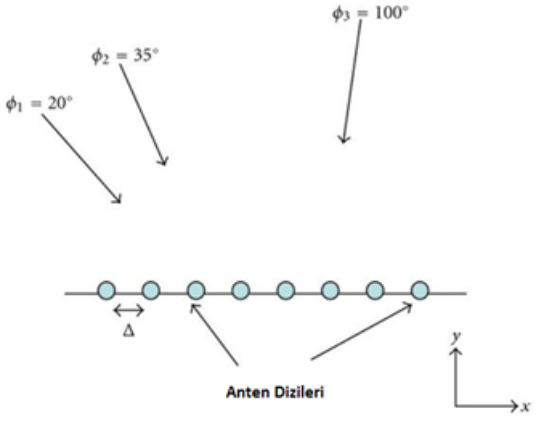
GPS Aldatma-Sinyal Karıştırma Saldırıların GPS Sinyal Geliş Doğrultusu (DOA) ile Tespiti

4.1 GPS ve DOA Algoritmaları

GPS GNSS sistemi üzerinde yapılan saldırılar GPS sinyal karıştırma ve GPS aldatma saldırıları olarak ikiye ayrılır. Bu iki saldırının tespitinde de GPS sinyal geliş doğrultusu (DOA) tespiti kilit önemdedir. GPS uyduları efemeris verilerini doğrultusunda farklı noktalardan yayın yapmaktadır. Hem aldatma saldırısında hem de karıştırma saldırısında tek yönden bir sinyal kaynağı ile saldırı yapıldığından tüm sinyallerin geliş doğrultusu aynı olacaktır ve bu ortak özellikleri ile iki saldırının da tespiti yapılabilmektedir. DOA kestirimin temeli gelişmiş anten yapıları kullanılarak, iletişim trafiğinin fazla olduğu bölgelerde, kısıtlı frekans aralığının etkin kullanılmasını sağlamaktır [46].

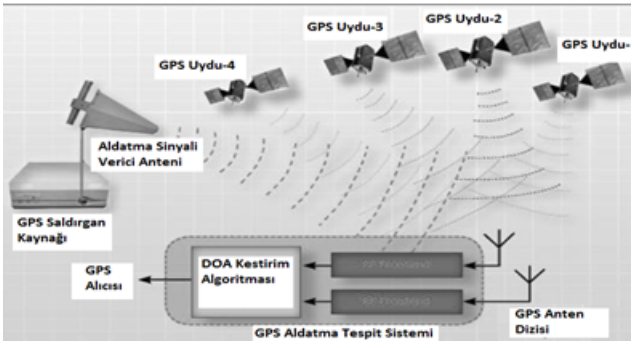
DOA tespiti aldatma saldırısı tespitinde kullanılan temel yöntemlerden biridir. Kullanılan anten sayısı, anten dizilimi, kullanım yerine göre boyut kısıtları, performans, uygulanabilirlik-komplekslik ve hassasiyet gibi bazı kriterler göre kullanılan algoritmalar farklılık göstermektedir. MUSIC (Multiple Signal Classification), Maximum likelihood, SAM (iterative Sparse Asymptotic Minimum Variance), Root-MUSIC, ESPRIT, CAPON yöntemleri başlıca DOA tespit algoritmalarıdır [47].

DOA kestiriminin GPS aldatma saldırısı tespit sistemi olarak kullanılmasıyla maliyet, hızlı işlem, boyut, yakın açı tespiti, çoklu kaynak tespiti, düşük SNR da yüksek başarım gibi konular diğer DOA uygulamalarına göre önem kazanmıştır. Aldatma saldırısı kaynağı ve gerçek GPS uydularının hepsini sinyal kaynağı olarak hesaba katıldığında çoklu ve birbirine yakın sinyal kaynaklarının sayısı artmış ve bu kaynakların tespit problemi için bu tez kapsamında başlıca parametreler ve algortimalar işlenip en uygun olanı bulunmaya çalışılmıştır.



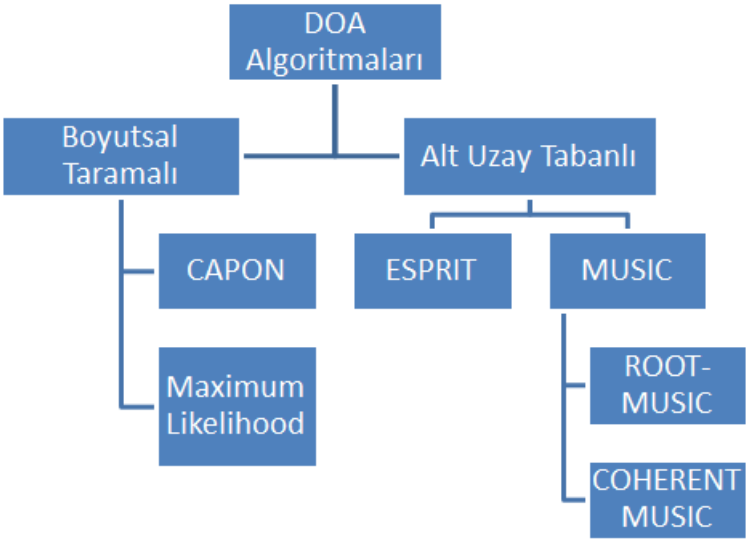
Şekil 4.1: DOA Tespiti İçin Belli Aralıklarla Dizilmiş Anten Dizileri

GPS aldatma saldırısında da tek yönlü bir kaynaktan uydu sinyallerinin hepsi basılacağından Şekil 4.2'deki gibi oluşan anomeli kolayca tespit edilebilmektedir; Ayrıca uydu efemeris bilgileri GPS alıcıda vardır. Eldeki bu verilerle de karşılaştırılırsa aldatma saldırısı tespit edilebilir.



Şekil 4.2: DOA ile Aldatma Saldırısı Tespiti

DOA kestirim yöntemleri kendi içinde tek antenli çözümler, çoklu antenli çözümler, anten dizilimlerine göre çözümler, işaret modelli, geleneksel yöntemler (gecikme ve toplama yöntemi), korelasyon- altuzay temelli yöntemler olarak çokca farklı alt gruplara ayrılır [48].



Şekil 4.3: DOA Metotlarının Listelenmesi [31]

MUSIC algoritması özdeğerler yönteminden biridir ve giriş kovaryans matrisinin öz değerlerini kullanan, yüksek çözünürlüğe sahip çoklu işaret sınıflandırma yöntemidir. MUSIC DOA algoritmasının temeli olan öz-analiz hesabı tekniği ise DOA işaretlerin zaman içindeki ortalamalarının alınması temeli vardır. Hassas ve doğru bir dizi kalibrasyonu, uygun parametrelerin belirlenmesi ile MUSIC algoritması çok yüksek çözünürlük sağlamaktadır [49].

ESPRIT DOA algoritması, MUSIC DOA algoritmasının olduğu gibi alt uzay tabanlı bir DOA algoritmasıdır. İki eş uzunlukta özdeş alt diziye bölünebilen bir yapısı vardır. Bu alt dizilerin parçaları arasındaki aralık sabittir. Alt dizi arasındaki delta yer değiştirme vektörünü referans yön olarak kullanarak işaret geliş açısı kestirme temeline dayanmaktadır. Bu nedenle ESPRIT algoritması dizi örüntüsüne ve uzay spektrumunun tamamen taranmasına ihtiyaç duymamaktadır ve MUSIC algoritmasına göre daha hızlı ve uygulanabilir olmaktadır [50].

Maksimum olabilirlik (ML) metodu, DOA kestirimi için geliştirilen ilk yöntemlerden biridir. Alt uzay tabanına dayanan yöntemlerle karşılaştırıldığında kestirim yükü ağır olduğundan çok kullanılmaz; ancak performans açısından kıyaslandığında, özellikle düşük SNR durumunda veya sinyal işaret örnekleri sayısı, çok fazla olmadığında alt uzay tabanlı yöntemlere göre başarıları vardır.

CAPON yöntemi minimum varyans gecikme ve toplama yöntemi olarak anlatılan en güçlü sinyali belirli bir doğrultuya yöneltmeye ve o doğrultuya gelen sinyal gücün yönünü kestirmeye dayanmaktadır. Sadece tek işaret kaynağı varlığında bu DOA algoritması başarılıdır; ancak çoklu işaretin olduğu durumunda, istenmeyen işaretler de dizi çıkış gücüne ekleneceğinden çözünürlük bozulmaktadır. Bu yöntemle çıkış sinyal gücü azaltılarak istenmeyen işaretler uzaklaştırılır, istenen yöndeki kazanç ise sabit kalır; ancak GPS aldatma gibi saldırı tespitinde çok sayıda kaynak olacağından aldatma tespitte çok başarılı bir yöntem değildir [51].

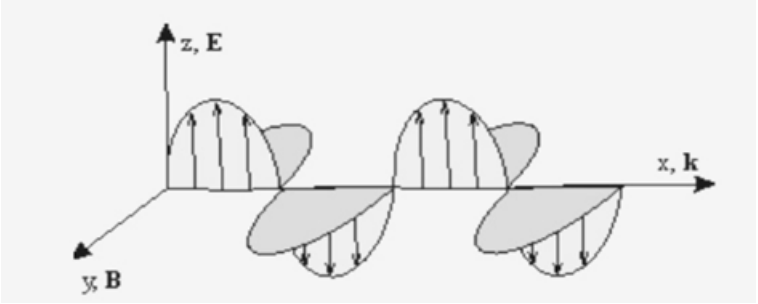
MUSIC DOA algoritmasının çözünürlük verimini arttırmak ve hesap zorluğunu azaltmak için algoritmada birtakım değişiklikler yapılmıştır. Bu değişikliklerden biri de Root-MUSIC algoritmasıdır. Bu DOA algoritma, polinom köklerine dayanmaktadır ve yüksek verim sağlamaktadır, ancak sadece düzgün aralıklı ULA diziler için verimlidir. MUSIC algoritmasının çoklu anten çözümlerinde işlevsel zorluklarını gidermiştir. Düşük SNR'lı sinyallerde yön tayininde Root-MUSIC daha başarılıdır. Tablo 4.1'da DOA algoritmalarının karşılaştırması gösterilmektedir.

Tablo 4.1: DOA Algoritmaları Karşılaştırması [52], [53]

Algoritma	Çözünürlük	Komplekslik	Hesaplama Yöntemi
Maximum Likelihood	Orta	Zor	M-Boyutlu tarama
CAPON	İyi	Orta	1-Boyutlu tarama
MUSIC	Çok İyi	Zor	Öz-Değerlere Ayrışım, 1-Boyutlu tarama
ESPRIT	Çok İyi	Orta	Öz-Değerlere Ayrışım
Root-MUSIC	Çok İyi	Orta	EVD, polinomsal

4.2 Temel Elektromanyetik Bilgileri ve Küresel Koordinat Sistemi

Elektromanyetik dalgalar, birbirine dik ve birlikte değişen elektrik ve manyetik alanların ivmeli hareket etmesiyle oluşur. Elektrik alan E ve manyetik alan B olarak ifade edilir.



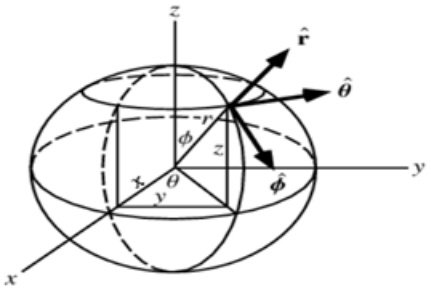
Şekil 4.4: Elektrik Alan ve Manyetik Alan Gösterimi

Elektromanyetik dalgaların oluşumunu Maxwell yasaları ile açıklanmıştır[54].

E= c.B

c= f . λ

Heinrich Rudolf Hertz, radyo dalgalarının laboratuar ortamında yayılmasını ve toplanmasını gözlemleyebilen ilk kisidir. Maxwell yasalarını doğrulamış ve elektromanyetik dalgaların hayatımızda bu kadar önemli noktalara gelmesini sağlamıştır.



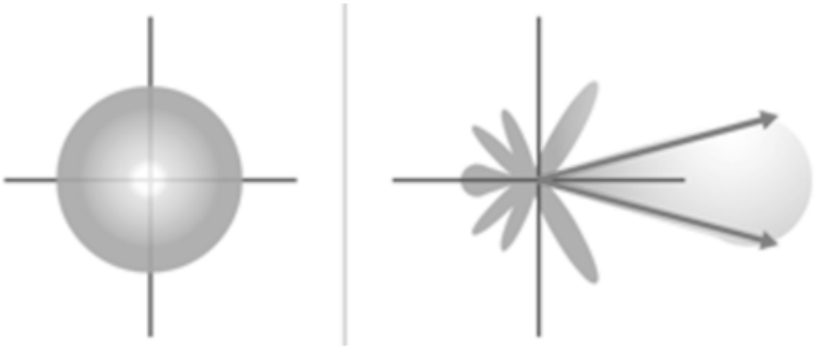
Şekil 4.5: Küresel Koordinat Sistemi

Elektromanyetik dalgalar taşıyıcı ortamı uzay ve alıcı-verici kanalları antenler olan dalgalardır. Bu dalgaların üretilmesinde ve alınmasında antenler kullanılır. Bu sinyaller antenler tarafından zaman girdisiyle birlikte 4 boyutlu uzayda temsil edilir s(x, y, z,t). Kutup açısını (zenit açısını) ve azimut açısını küresel koordinat sistemine göre karşılıkları belirtilmiştir. Zenit açısı 0-180 derece arasında, azimut açısı ise 0-360 derece arasında hareket eder. Böylelikle birbirine dik iki eksende ifade edilen kutup açılarıyla bir kürenin

tüm noktaları elde edilmiş olunur.Küresel koordinat hesaplarından kutup açısı, azimut açısı, x,y,z,r hesaplamaları yapılarak elektromanyetik vektör hesapları bulunur.

Anten, uzay ile iletim hattı arasında elektromanyetik işaret geçişini sağlayan elektronik elemanıdır. Antenler elektromanyetik dalgaları göndermek veya almak için kullanılan cihazlardır. Anten tekli yapıda kullanılabildiği gibi (farklı boyut ve uygulamalarda), çok sayıda anten birleştirilerek dizi sırasında (array) kullanılabilir. Antenler ışıma ve alma doğrultuları özelliklerine göre her yönde eşit ışıma yapan tiplerine yönsüz (omnidirectional) antenler ve sadece tek yönde diğerlerine göre daha fazla ışıma yapan yönlü (directional) antenler olarak ayrılır[55].

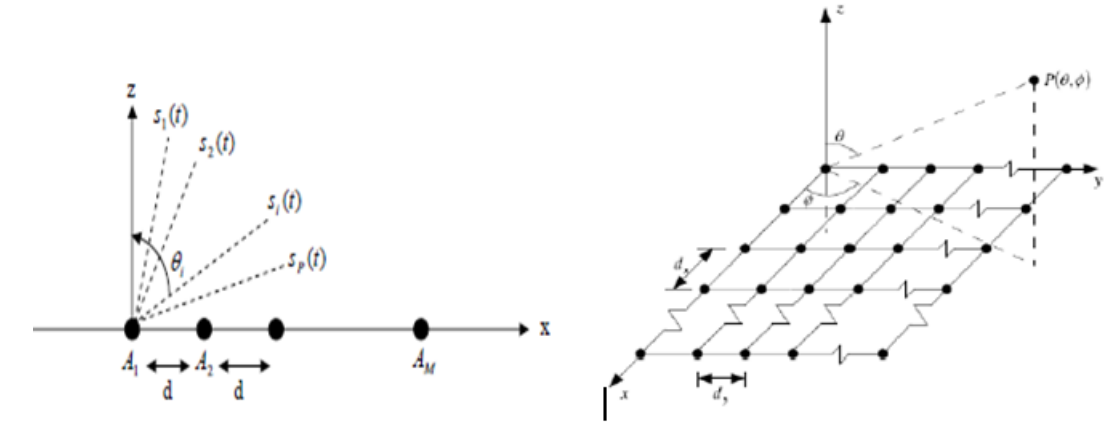
Yönsüz antenler, uzaya yaydığı EM dalga şiddeti tüm yönlerde eşit olan antenlerdir. Belli bir yöne odaklanılmaksızın, ışıma gücü tüm yönlere eşit olarak yayarlar. Yönlü antenler, EM dalgayı belirli bir yönde diğer yönlere göre daha etkili olarak yayan veya alan anten gruplarıdır. Verimlilik açısından yönlü antenler kullanılmaktadır[55].



Şekil 4.6: Yönsüz ve Yönlü Anten Işıma Analizi

Tek bir antenin ışıma örüntüsü incelendiğinde, hüzme açıklığının geniş olduğu ve yönelticiliğinin az olduğu görülmektedir; ancak uzak mesafeler ile haberleşme gerektiren durumlarda, DOA veya radar uygulamalarında anten gücünün istenen bir doğrultuda yoğunlaştırılması beklenmektedir. Tek bir antenin bu ihtiyacı karşılamaması nedeniyle çoklu anten dizilerine geçilmiştir. Birden fazla anten belirli şekillerde birlikte kullanılarak istenen anten gücü sağlanmıştır. Bu tip birden fazla antenin belli bir geometrik şekilde bir araya getirilmesi ile oluşan anten yapılarına anten dizileri denir. Anten dizileri 1 veya 2 boyutlu olabilirler. Doğrusal Anten Dizileri: Anten dizileri içerisinde en basit

ve en pratik olanı bir doğru üzerine yerleştirilmiş elemanlardan oluşan doğrusal anten dizileridir. Her bir dizi kendi dizi faktörüne sahiptir. Bu dizi faktörü genellikle, dizi eleman sayısının, geometrik dizilimin, elemanlar arasındaki boşluğun, faz ve genliğin bir fonksiyonu olarak ifade edilmektedir. Düzlemsel anten dizileri, dizi elemanlarının bir düzlem üzerine yerleştirilmesi ile oluşur. Düzlemsel anten dizilerinin doğrusal anten dizilerine göre en önemli avantajı, ışıma örüntüsünün uzayda iki boyutlu tarama yapabilmesidir. Doğrusal anten dizileri sadece kendi bulunduğu düzlemde uzayı tarayabilirken, düzlemsel diziler bulunduğu düzlemde iki boyutlu tarama yapabilmekte ve ışıma hüzmesini iki boyutlu olarak yönlendirebilme imkanı sunmaktadır.



Şekil 4.7: Doğrusal ve Düzlemsel Anten Dizilimleri

4.3 İlgili Çalışmalar

Tezin içeriğini belirlemeden önce literatür taraması yapılıp benzer araştırmalar bulundu. GPS aldatma saldırısı üzerine çalışmanın ilk adımı olarak GPS sistemin temelleri araştırıldı ve karşılaşılmış sorunlar incelendi. Bu adım doğrultusunda standartlar [3] ve GPS altyapısı [56] üzerine çalışıldı. Güvenlik sorunları ve bunlar üzerine yapılan yayınlar incelendiğinde [57]'de kompleks saldırılar anlatılmıştır, [58]'de ise düşük bütçe ve komplekslikteki saldırılar incelenmiştir. Literatürde GPS sistemine yapılan saldırıları konu edinen yayınlar listelendi ve en çok atıf yapılan çalışmalar bulundu. [59]'da GPS üzerine yapılan saldırı yöntemi olan GPS sinyal karıştırma saldırısı ayrıntılı olarak anlatılmıştır ve

uygulama kısmında yapacağımız saldırı senaryosu bu çalışmalar gözönüne alınarak oluşturuldu.

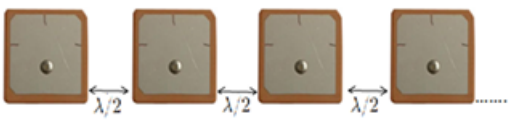
GPS saldırıların yapılış kısmı bitirildikten sonra bu saldırılara karşı önlem ve tespit kısmına geçildi. [45] ve [60]'da GPS saldırılarına karşı tespit yöntemleri anlatılmış ve bu yöntemler karşılaştırmıştır. Bu karşılaştırmalar sonucu saldırı tespit yöntemleri kompleksliğuygulanabilirlik, başarım performansı, yöntem temelleri gibi kategorilere göre sınıflandırılmıştır. Saldırı çeşitleri ve önlemler araştırıldıktan tezin uygulama kısmına geçildi. Literatür araştırmasının verdiği bilgiler doğrultusunda DOA saldırı tespit yönteminin hem sinyal karıştırma hem de aldatma saldırında kullanılabilecek bir yöntemi olduğu belirlendi ve uygulama kısmı için tercih edildi.
[49] ve [61]'de DOA kestirim yöntemleri anlatılmıştır.Bu çalışmalar incelenerek GPS saldırılarının karakteristik özellikleri özelinde en uygun algoritmayı bulmak amaçlanmıştır. [62] ve [48]'de DOA performansları anlatılmıştır. Bu çalışmalarda bulunan sonuçlar ile tez kapsamında elde edilen sonuçlar karşılaştırılmıştır.
DOA algoritmalarını ve GPS üzerine yapılan saldırıları inceledikten sonra tezin uygulama kısmı olan DOA ile GPS aldatma saldırısı tespiti üzerine literatür araştırması yapıldı. [63] ve [64]'de DOA ile GPS aldatma saldırıların tespiti anlatılmıştır. Bu çalışmalar incelendikten sonra daha kompleks ve çoklu kaynaklı saldırıların tespiti üzerine odaklanmaya ve DOA ile saldırı tespit başarımını artırmak için kullanılan tüm parametrelerde optimizasyon yapılmasına karar verildi.

Bölüm 5

DOA ile GPS Aldatma Saldırısı Tespiti MATLAB Uygulaması

5.1 MATLAB DOA Uygulamasına Giriş

Aldatma saldırı senaryosu için öncelikle gerçek GPS verilerine ihtiyacımız vardır. Burada GPS alıcılı cep telefonuna (SM-N935F/DS) yüklenilen uygulama (NMEA Tools, Version 1.8.2) ile üzerindeki GPS alıcısı kullanarak veri setleri elde edilmiştir. GPS sinyalleri L1 1575,42MHz, L2 1227,6 MHz, L5 1176,45MHz frekansları üzerinden yayın yapar. L1 için 19,05cm, L2 için 24,45cm ve L5 için 25,48cm dalga boyuna sahiptir. Konum verisi, yayınlanma sıklığı ve dalga boyu nedeniyle L1 frekansı DOA tespitinde kullanılmaktadır. Şekil 5.1'de gösterildiği gibi GPS antenleri ULA (Düzgün Doğrusal Dizilim) diziliminde yarım dalga boyu aralıklarla dizilip uygulama bunun üzerinden yapılmıştır.



Şekil 5.1: GPS Anten Dizisi Uygulaması

Cep telefonuna (SM-N935F/DS) yüklenilen uygulama (NMEA Tools, Version 1.8.2) ile NMEA verilerine ulaşılır.NMEA(National Marine Electronics Association) veri standartıdır ve içeriği Tablo 5.1'de verilmiştir.

Tablo 5.1: GPGSV Paket Yapısı

AAM	Waypoint Arrival Alarm
ALM	Almanac data
APA	Auto Pilot A sentence
APB	Auto Pilot B sentence
BOD	Bearing Origin to Destination
BWC	Bearing using Great Circle route
DTM	Datum being used
GGA	Fix information
GLL	Lat/Lon data
GRS	GPS Range Residuals
GSA	Overall Satellite data
GST	GPS Pseudorange Noise Statistics
GSV	Detailed Satellite data
RMA	Recommended Loran data
RMB	Recommended navigation data for gps
RMC	Recommended minimum data for gps
RTE	Route message
TRF	Transit Fix Data
STN	Multiple Data ID
VBW	Dual Ground / Water Spped
VTG	Vector track an Speed over the Ground
WCV	Waypoint closure velocity (Velocity Made Good)
WPL	Waypoint Location information
XTC	Cross track error
XTE	Measured cross track error
ZTG	Zulu (UTC) time and time to go (to destination)
ZDA	Date and Time

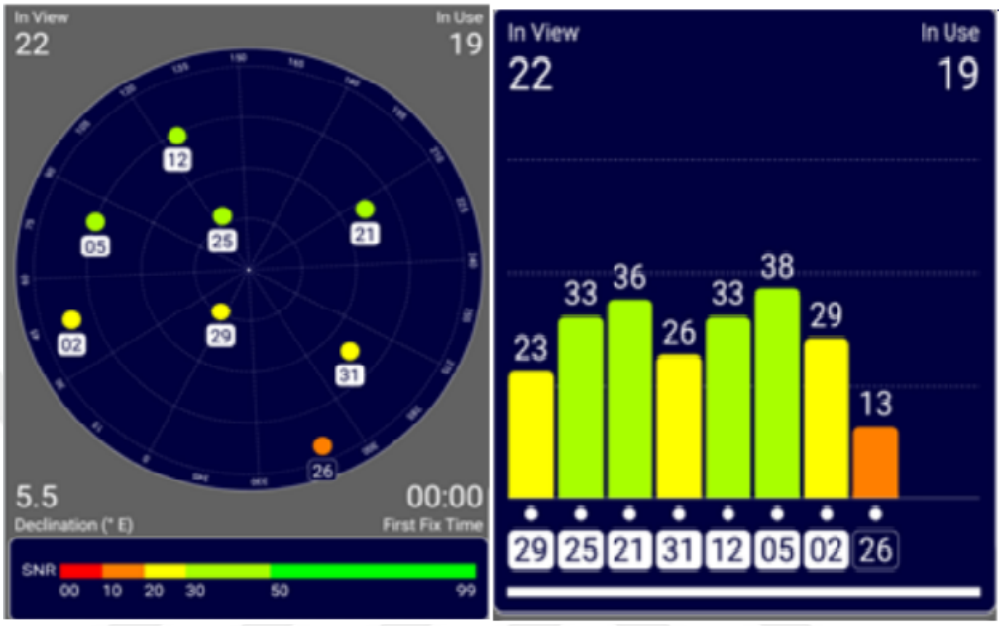
Burada GPS uyduları ile ilgili bilgiyi veren parametre GSV parametresidir ve bu parametreye Tablo 5.2'de ayrıntılı bakıldığında ise görülen uydu sayısı, PRN numaraları, elevation ve azimuth açıları, SNR kuvvetleri gibi değerlere ulaşılmaktadır.

Tablo 5.2: GSV Paket Yapısı

$GSV,1,2,3,4,5,6,7,8—11,12—15,16—19	
1	Total number of messages of this type in this cycle
2	Message number
3	Total number of SVs in view
4	SV PRN number
5	Elevation in degrees, 90 maximum
6	Azimuth, degrees from true north, 000 to 359
7	SNR, 00-99 dB (null when not tracking)
8-11	Information about second SV, same as field 4-7
12-15	Information about third SV, same as field 4-7
16-19	Information about fourth SV, same as field 4-7

Cep telefonu (SM-N935F/DS) ve yüklenilen uygulama (NMEA Tools, Version 1.8.2) ile 30 dakikalık veriler alınır, GSV verileri işlenir ve her uydu için anlık açı değerlerine

ulaşılır. Kayıtları alınan 40.979406, 29.128126 konumu saat 19:00-20:00 arasındaki GPS uydu konumları, ID ve SNR değerleri Şekil 5.2'de gösterilmiştir.



Şekil 5.2: Alınan GPS verilerine ait GPS Uyduları ve SNR Değerleri

Bu işlemler sonucu İstanbul Ataşehir (40.979406, 29.128126) konumunda saat 19:00-20:00 arasındaki GPS uydu konumları elde edilir. Alınan GSV verilerinden GPS uydularına ait açı verileri bulunur. Tablo 5.3'de bulunan gerçek GPS değerleri üzerinden tüm saldırı senaryolar yapıldı.

Tablo 5.3: İşlenen GPGSV Verisinden Elde Edilen Veriler

GPS Uydu ID	Azimuth	Elevation	SNR
12	123	33	34
21	212	32	25
25	119	72	33
29	353	71	18

Tez çalışması kapsamında incelenecek GPS aldatma saldırısı senaryoları için kullanılacak sanal GPS aldatma saldırısı kaynağına ait açı bilgileri Tablo 5.4'de verildi. Bu saldırı senaryosu ile tek kaynakta 4 tane aldatma saldırısı sinyal çıkışı olacaktır. Tüm saldırı senaryoları, 4 gerçek ve 4 sanal toplam 8 kaynağın DOA hesaplamaları üzerinden yapılmıştır.

Tablo 5.4: Oluşturulan Aldatma Saldırısı Kaynağına Ait Veriler

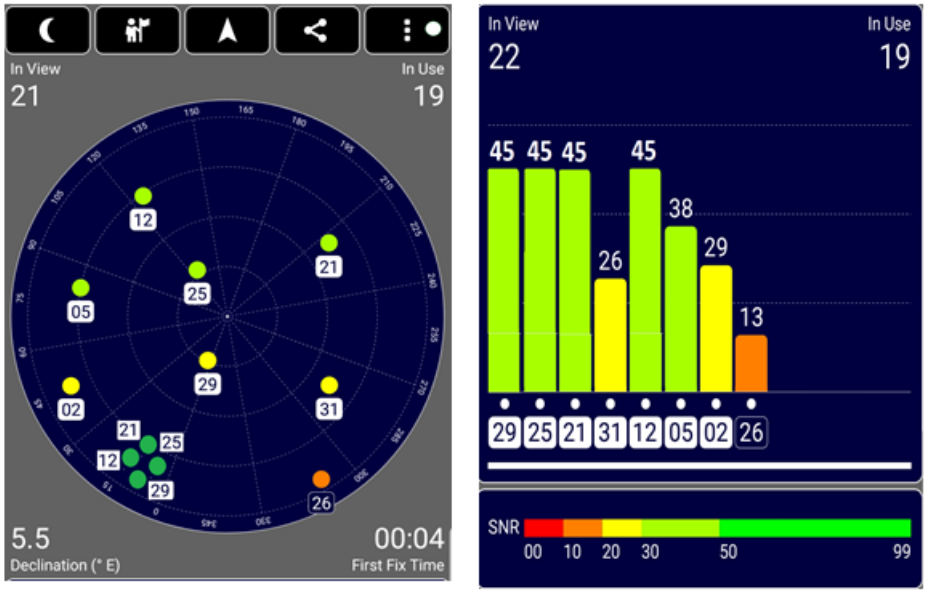
Spoofing ID	Azimuth	Elevation	SNR
X	10	53	50

MATLAB DOA algoritmalarının testlerinde gerçek ve sanal GPS sinyal kaynaklarının açıları broadside cinsinden girilmesi gerekmektedir.Bu nedenle DOA algoritmalarında kullanılacak broadside açıları da hesaplanıp Tablo 5.5'de verilmiştir.

Tablo 5.5: Hesaplanan Broadside Açı Değerleri

Uydu ID	Hesaplanan Broadside Açısı
12	44.6978
21	-26.7050
25	15.6804
29	-2.2739
Spoofing	5.9985

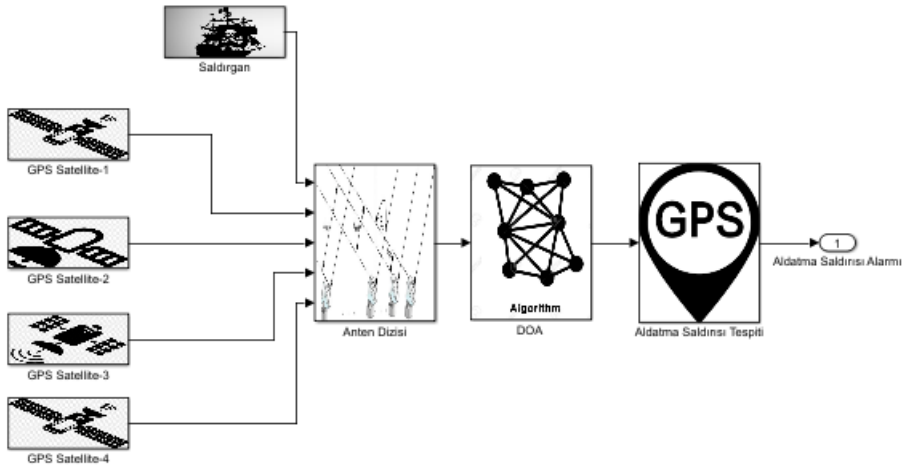
GPS aldatma saldırısı sonucunda elde edilecek temsili GPS uydu konum haritası Şekil 5.3'de gösterilmiştir. GPS aldatma saldırısı tek kaynaktan yapılacağı için burada 12,21,29 ve 25 ID'li uyduların tek bir noktada ve eşit SNR değerinde kümelendiği görülür.



Şekil 5.3: Aldatma Saldırısı Kaynağı ile Yeni Oluşacak Uydu Görüntülerinin Temsili Gösterimi

5.2 GPS Aldatma Saldırısı DOA Tespit Tabanlı Alarm Modeli

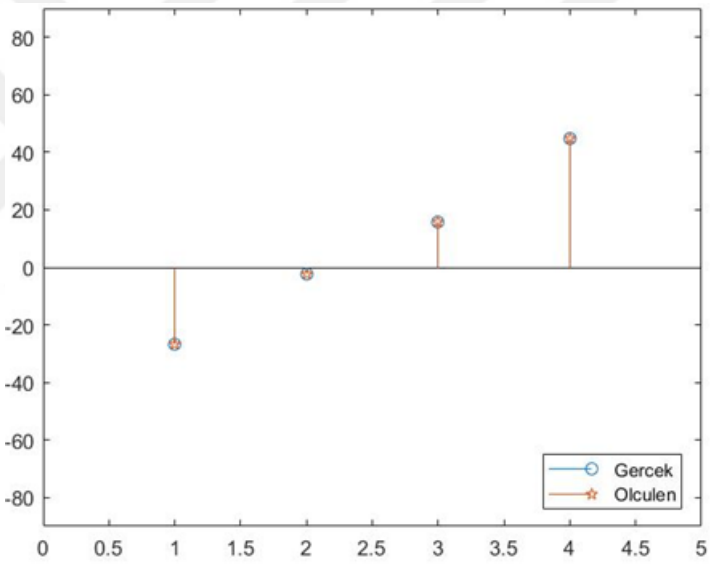
GPS aldatma saldırısı MATLAB tespit modelinde toplam açı farkından saldırı tespiti yapılacaktır. Şekil 5.4'de 4 gerçek GPS uyduları ve saldırgan sinyallerin ULA anten dizisine girişi ile başlar. Broadside açıları ve diğer parametreler de hesaplanır DOA algoritma kısmına girilir. Burada DOA algoritmaları kullanılarak açı konumları hesaplanır. Efemeris verilerinden hesapladığımız açı değerleriyle hesapladığımız arasındaki açıların toplam farkı 20 derece ve üssü olduğunda GPS aldatma saldırısı alarm oluşturur. GPS aldatma saldırı tespit toleransı istenilen hassasiyete göre ayarlanır. Kullanılan donanımın yeteneklerine göre hata eşik oranları azalır ve karmaşık saldırıların tespitini sağlar. GPS alıcısının toplam açı ölçüm hata oranı, çok sayıda kaynak olması durumunda 5-8 derecelere kadar çıkabilmektedir. Bu tez kapsamında alarm eşik değeri 20 derece alınmıştır. Kaynakların tek açıdan gelmesi üzerine yapılan GPS aldatma saldırısı tespitinde ise birbirine en yakın 4 geliş açısında arasındaki fark 10 dereceden az ise saldırı tespiti yapılabilmektedir.



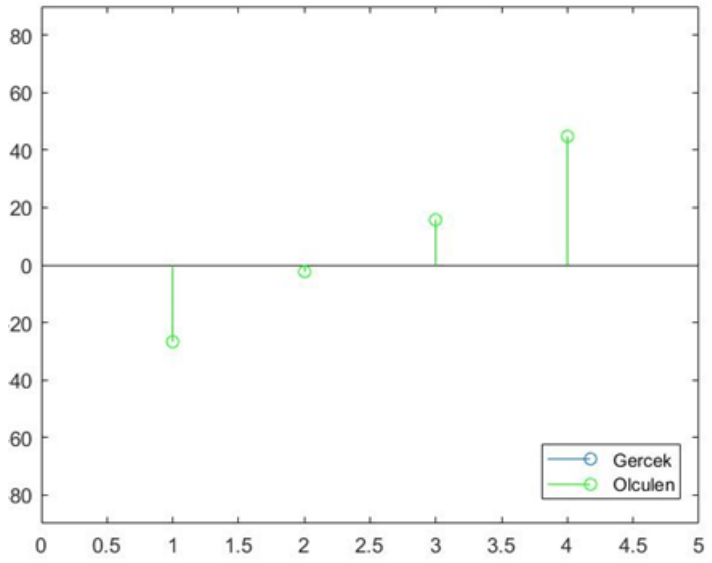
Şekil 5.4: MATLAB Simulink Saldırı Tespit Modeli

5.3 Aldatma Saldırısı Öncesi DOA Tespit Başarısı

GPS aldatma saldırısı öncesi DOA algortimalarının başarısını test etmek için elimizdeki veri setleri ile 4 GPS uydusu ve onların açı değerleri bulundu. Bu çalışma boyunca çizilen grafiklerde x ekseni sinyal kaynağının numarasını y ekseni ise geliş açısının broadside cinsinden değerini göstermektedir. 4 kaynak üzerinden yapılan açı tespitinde ölçülen ve gerçek değerler üstüste çizildi ve çok az hata ile kaynaklar bulundu. Aldatma saldırısı öncesi SNR:40 Anten Sayısı:20 Örnek Sayısı: 6 iken Root-MUSIC toplam hatası 0,005 ESPRIT toplam hatası 0,003 ile Şekil 5.5 ve Şekil 5.6'de gösterildiği gibi 4 GPS uydusu sinyal geliş açıları hesaplandı.

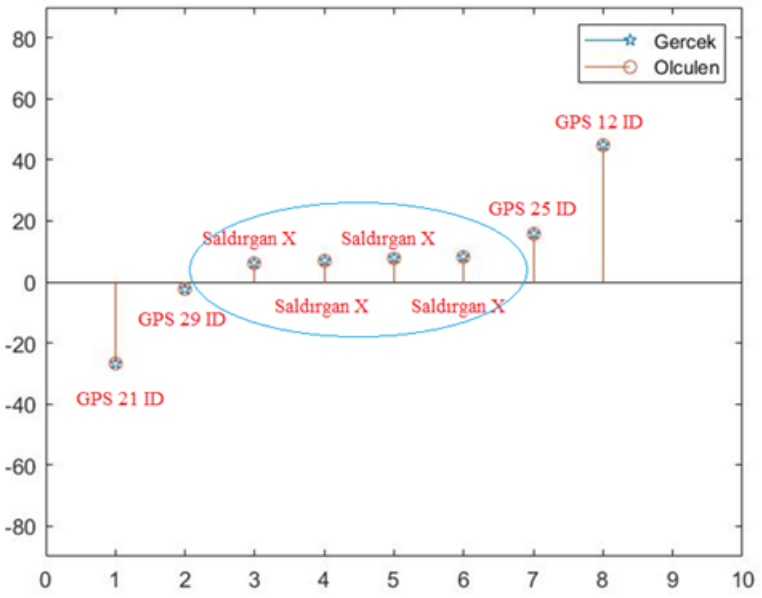


Şekil 5.5: Aldatma Saldırısı Öncesi Root-MUSIC ile Toplam 0,005 Hatalık DOA Tespiti



Şekil 5.6: Aldatma Saldırısı Öncesi ESPRIT ile Toplam 0,003 Hatalık DOA Tespiti

GPS aldatma DOA performans testleri MATLAB uygulamasında Şekil 5.7'de gösterildiği gibi 12, 21, 25, 29 ID'li GPS uyduları ve aynı açılı 4 adet GPS aldatma saldırısı sinyal kaynağı broadside açılarının gösterimi yapıldı. Tüm hesaplamalarda bu gerçek GPS ve GPS aldatma saldırısı kaynakları gerçek ve ölçülen değerlerinin üstüste çizilmesiyle ve toplam açı hata farklarının hesaplanmasıyla yapıldı.



Şekil 5.7: GPS Uyduları ve Aldatma Saldırı Sinyal Kaynaklarının Geliş Açılarının Gösterimi

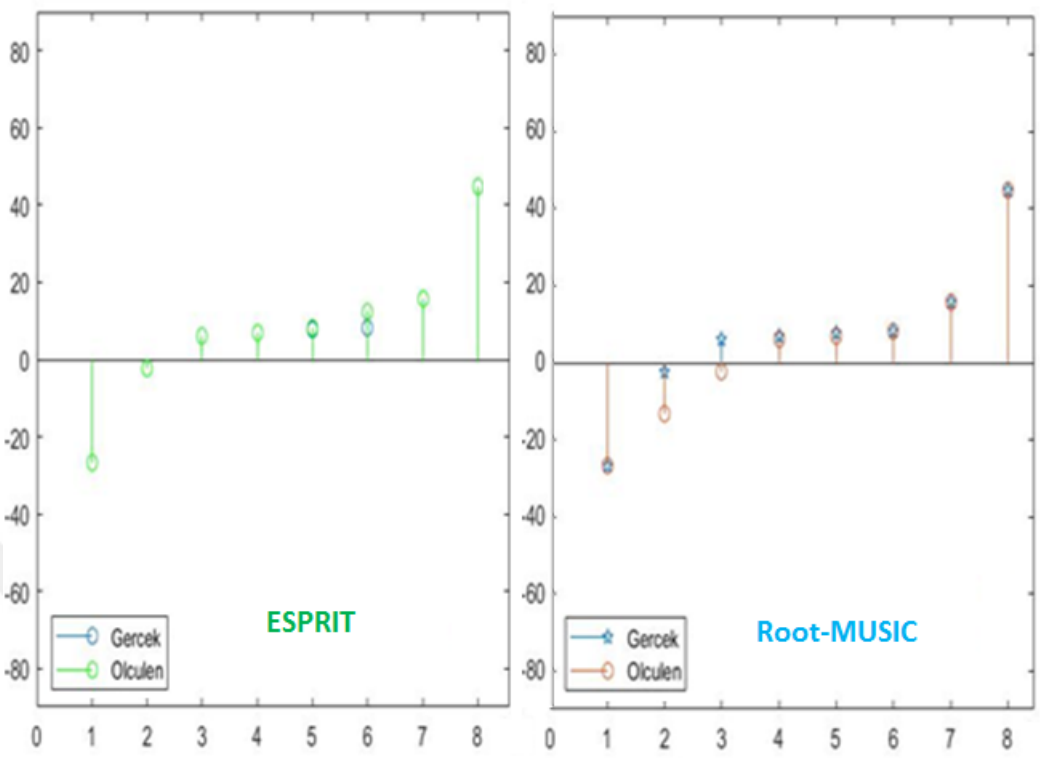
5.4 Örnek Sayısı Farklılığında DOA Performansları

Tezin bu bölümüde GPS saldırı tespit modelinde kullanılan parametrelerin DOA tespit başarılarına olan etkisi incelenmektedir. Gün içinde uyduların hareketleri sonucu uydu açıları birbirine yaklaşır ve uzaklaşır. Bu nedenle saldırgan yeri tespiti için çok daha hassas ölçüm yapmak gerekir. İlk parametre örnek sayısının artırılmasıdır. SNR=40, Anten Sayısı=20 tutularak Örnek Sayısı=4 ile başlayan ve 100 örnek sayısına kadar Root-MUSIC, ESPRIT algoritmaları uygulanmıştır ve aldatma saldırı tespiti yöntemi olarak yapılan hesaplamalar Tablo 5.6'de verilmiştir. Hata payı tüm sinyal kaynaklarının (gerçek ve sanal GPS uyduları) gerçek ve ölçülen açı değerleri arasındaki toplam farkını vermektedir.

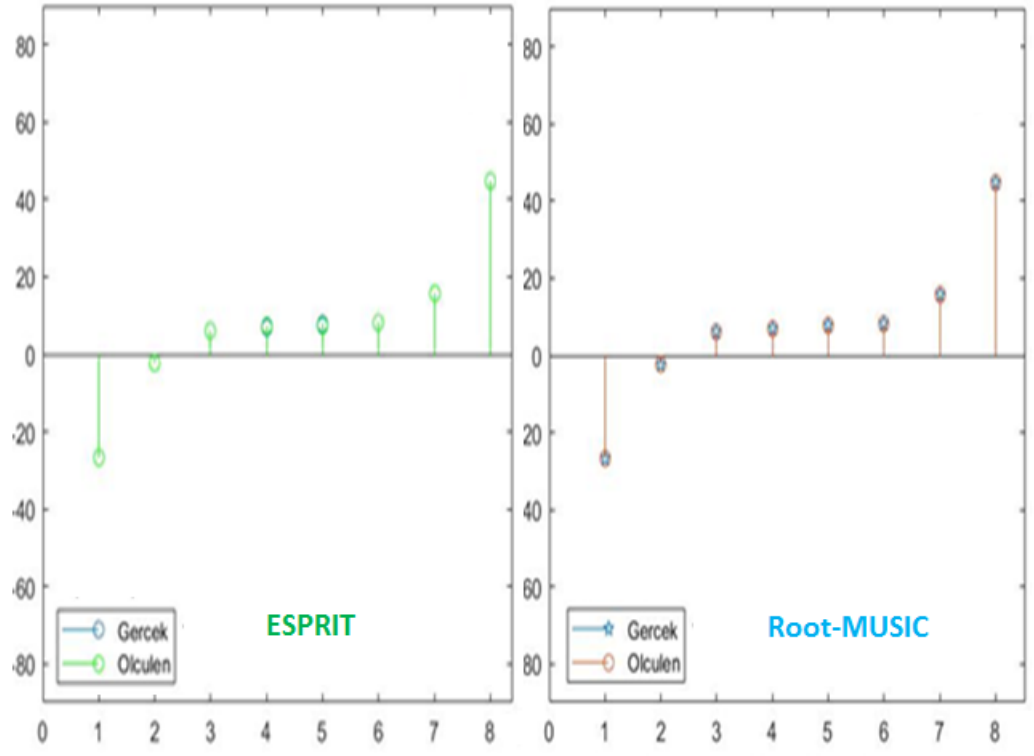
Tablo 5.6: Örnek Sayısı Açısından ESPRIT ve Root-MUSIC Karşılaştırması

Ornek Sayısı	ESPRIT (Toplam Hata)	Root-MUSIC (Toplam Hata)
4	25.0032	41.6220
6	5.0612	20.6260
8	1.4949	4.2042
16	1.5046	1.0259
30	1.1562	0.9866
100	0.7592	0.6315

Şekil 5.8'de Örnek Sayısı=6 üzerinde Şekil 5.9'de Örnek Sayısı=100 üzerinden hesaplamalar gösterilmiştir. Düşük örnek sayısında ESPRIT algoritmasının Root-MUSIC'e göre daha başarılı olduğunu ama örnek sayısının artığında ikisinin de çok başarılı olduğu gözlemlenmektedir. Burada örnekleme sayısının düşük olması düşük komplekslikte ve hızlı çözüm isterleri için istenen bir özelliktir. Yüksek örneklemede 2 metot arasında bir farklılık yoktur. Düşük örnekleme çözümlerinde [65]'de düşük maliyetli ve tek örnekleme ile yön tespiti yapmaktadır. Bu çalışmaları yakın gelecekte mobil araçların güç tüketiminde anten verimliliği çok önem kazanacağından değerlidir; ama bu çalışmalarında 1 ve 2 adet kaynak üzerinden yapıldığından bizim sistemimizde kullanılamaz. [49]'de yayınında da 4 kaynak üzerinden farklı örnekleme sayıları ile ESPRIT ve Root-MUSIC karşılaştırmaları yapılmış ve özellikle yüksek örneklemelerde benzer sonuçlara ulaşılmıştır. Bu çalışmada da 4 kaynak üzerinden toplam hata 0.01'in altındadır ve birbirine yakındır.



Şekil 5.8: ESPRIT & Root-MUSIC Örnek Sayısı=6 DOA Kestirimi



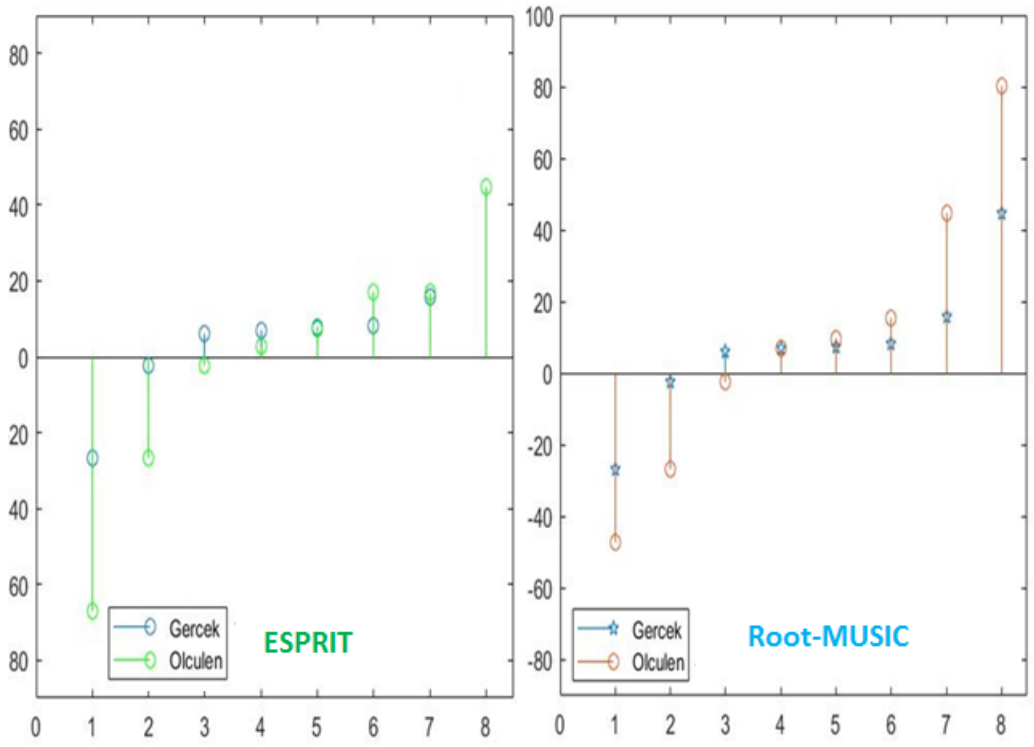
Şekil 5.9: ESPRIT & Root-MUSIC Örnek Sayısı=100 DOA Kestirimi

5.5 Anten Sayısı Farklılığında DOA Performansları

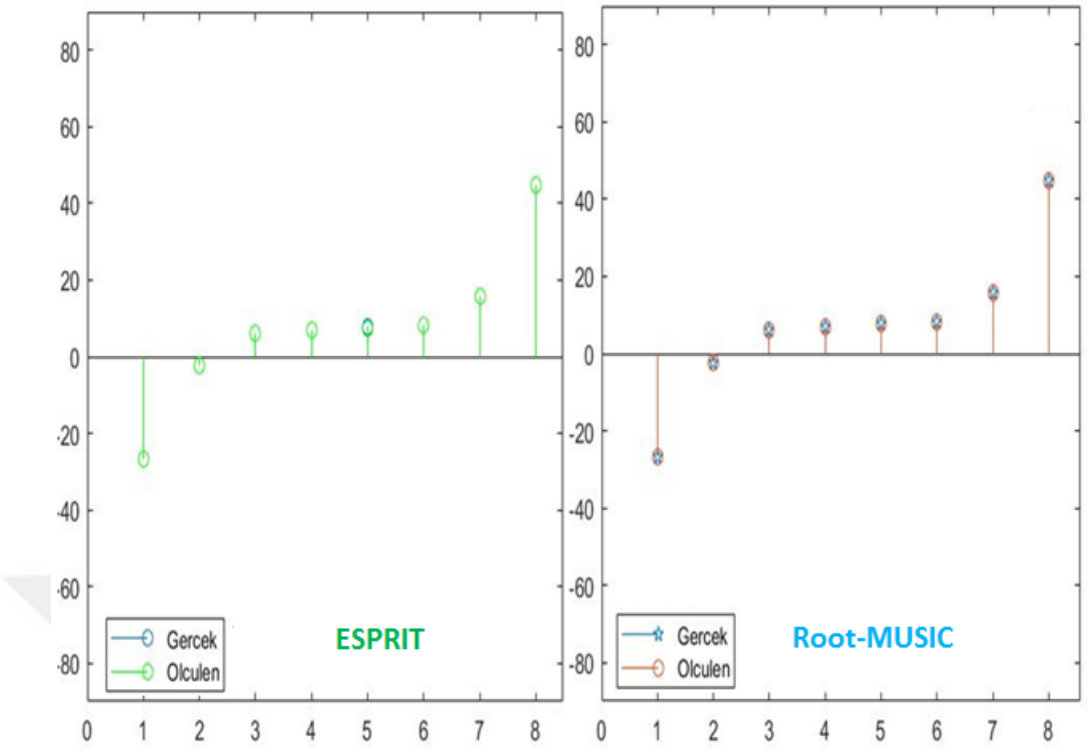
Örnek sayısından sonra ele alınacak ikinci parametre anten sayısıdır. SNR=20, Anten Sayısı=10 Örnek Sayısı=10 ile başlayan ve anten sayısı değerinin 100 'e kadar çıkarıldığı Root-MUSIC, ESPRIT algoritmalarının aldatma saldırısı tespiti yöntemi olarak DOA tespiti performansları Tablo 5.7'de verilmiştir.

Tablo 5.7: Anten Sayısı Açısından ESPRIT ve Root-MUSIC Karşılaştırması

Anten Sayısı	ESPRIT (Toplam Hata)	Root-MUSIC (Toplam Hata)
10	87.8841	127.2207
20	50.5468	51.2042
30	2.7643	6.9607
50	0.1976	0.1439
100	0.0130	0.0034



Şekil 5.10: ESPRIT & Root-MUSIC Anten Sayısı=10 DOA Kestirimi



Şekil 5.11: ESPRIT & Root-MUSIC Anten Sayısı=100 DOA Kestirimi

Şekil 5.10'de Anten Sayısı=10 üzerinde Şekil 5.11'de Anten Sayısı=100 üzerinden hesaplamalar gösterilmiştir. Burada düşük anten sayısında ESPRIT daha başarılıdır, anten sayısı arttıkça ikisi de çok iyi performans göstermektedir. Anten sayısı DOA tespitinde en önemli parametresidir; ayrıca kullanılacak anten sayısı oluşturulacak DOA tespit cihazının boyutunu belirleyecektir. Anten sayısı arttıkça boyut ve işletim zorlukları artacaktır. Bu durum sıkça saldırıya uğrayan hava araçları gibi sistemlerde kullanımında optimizasyonu zorunlu kılmaktadır. [2]'deki yayında da benzer bir konu işlenmiştir. Tespit edilecek 3 kaynak için 7,21,50,100 ve 200 anten sayılarında hesaplamalar yapılmıştır. -20,20,40 derecelik açı değerlerine sahip 3 kaynağın SNR=25dB, Örnek Sayısı=50 parametreleriyle MUSIC, Root-MUSIC ve ESPRIT karşılaştırmaları yapılmıştır. Bu karşılaştırmaya aynı parametre değerleriyle hesapladığımız GPS aldatma saldırısı senaryo sonuçları da eklenip Tablo 5.8'de gösterilmiştir. Çalışma sonuçlarıyla düşük anten sayısında ESPRIT ve Root-MUSIC algoritmasının iyi performans gösterdikleri görülmüştür. Bu örnekte tez kapsamında yapılan çalışmadaki kadar keskin farklılıkların olmamasının nedeni kaynak sayısının 3 adet olması ve birbirine çok yakın kaynaklar olmamasıdır.

Tablo 5.8: Anten Sayısı Etkisi Çalışması [2] ve GPS Aldatma Saldırısı Sonuçlarının Karşılaştırması

SNR=20dB, Örnek Sayısı=50				
Algoritma	Root-MUSIC*	ESPRIT*	Root-MUSIC**	ESPRIT**
Anten Sayısı	Toplam Açı Hatası	Toplam Açı Hatası	Toplam Açı Hatası	Toplam Açı Hatası
7	0,0466	0,0684	157,23	107,23
21	0,0180	0,0166	25,6494	2,6233
50	0,0014	0,0056	0,0279	0,0997
100	0,0010	0,0030	0,0022	0,0053
200	0,0005	0,0340	0,000247	0,00061

* [2] yayın sonuçları

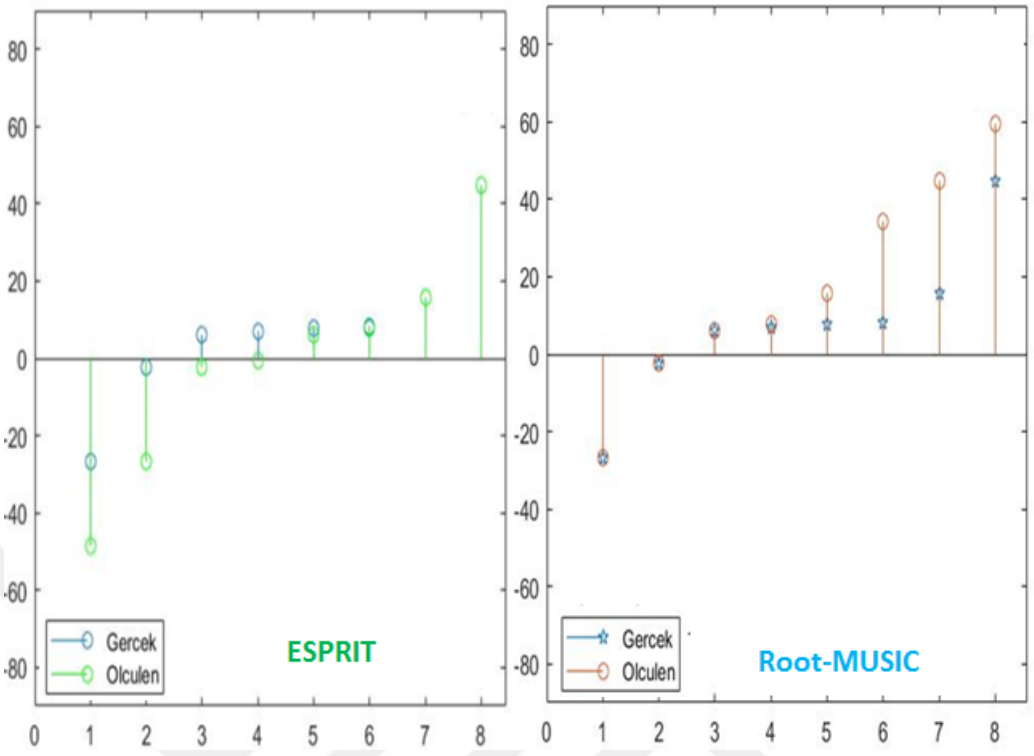
** GPS aldatma saldırı senaryosu sonuçları

5.6 SNR Değeri Farklılığında DOA Performansları

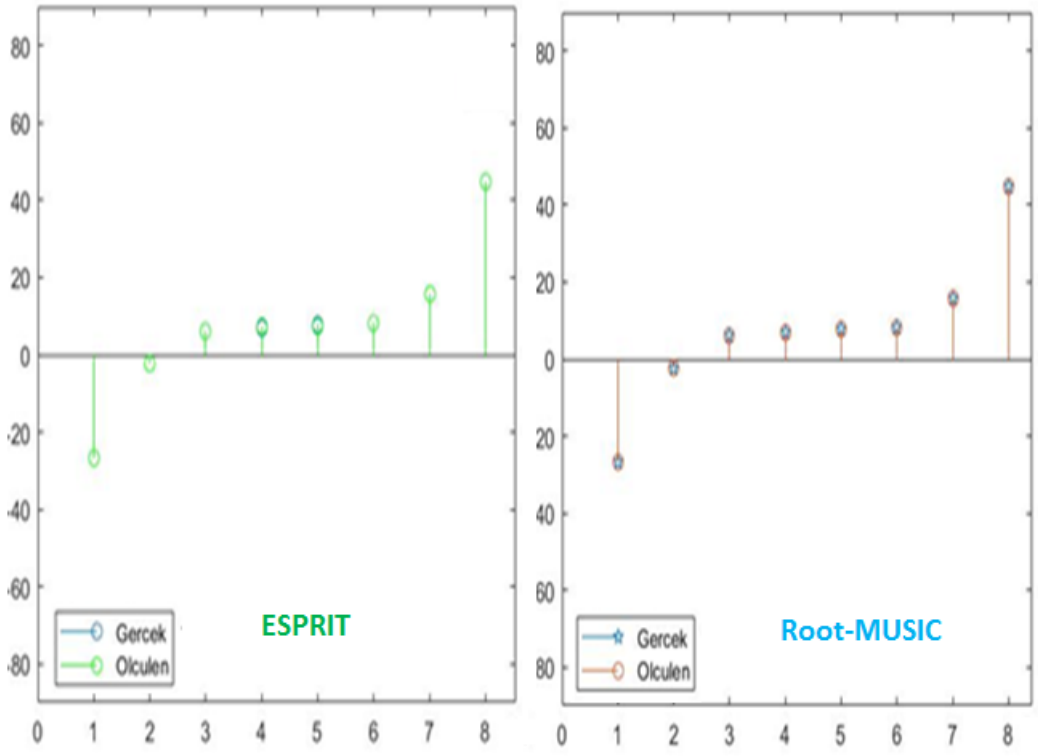
SNR değeri DOA başarım performansını etkileyen diğer önemli değişkendir. Düşük sinyal kuvvetinin olduğu durumlarda DOA tahmini zorlaşmaktadır. GPS aldatma saldırısı tespitinde GPS sinyal SNR değerin düşük olması uygun tespit yönteminin belirlenmesi ve parametre optimizasyonunu işlemlerini zorunlu kılar. SNR=0, Anten Sayısı=20, Örnek Sayısı=10 ile başlayan SNR değerinin 0'dan 50'e çıkarıldığı Root-MUSIC, ESPRIT algoritmalarının aldatma saldırısı tespit yöntemi karşılaştırmaları Tablo 5.9'deki gibidir. Şekil 5.12'de SNR=0 üzerinde ve Şekil 5.13 SNR=50 üzerinden hesaplamalar gösterilmiştir.

Tablo 5.9: SNR Değerleri Açısından ESPRIT ve Root-MUSIC Karşılaştırması

SNR	ESPRIT (Toplam Hata)	Root-MUSIC (Toplam Hata)
0	64.5882	79.0223
10	51.1804	70.1224
20	50.5468	51.2042
30	34.2013	21.1226
50	0.9518	0.3229

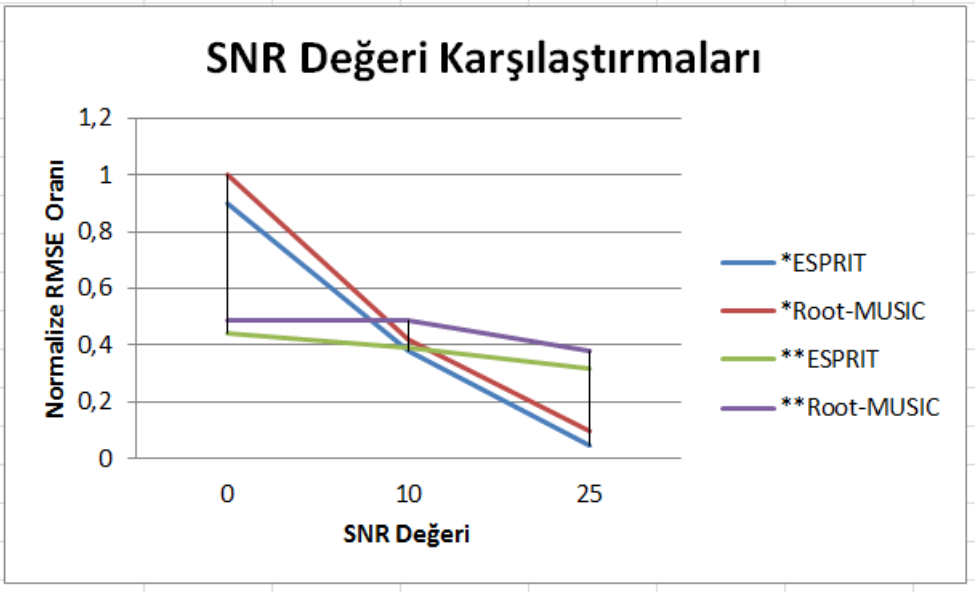


Şekil 5.12: ESPRIT & Root-MUSIC SNR=0 DOA Kestirimi



Şekil 5.13: ESPRIT & Root-MUSIC SNR=50 DOA Kestirimi

Düşük SNR değerinde ESPRIT, Root-MUSIC'e göre daha başarılı gözükmektedir; ancak SNR değeri artınca iki algoritmanın da performansı iyileşmektedir. Düşük SNR değerinde DOA tespiti GPS zayıf bir sinyal olduğundan önemli bir kriterdir. [1] yayınında yakın alanlı sinyallerin kaynak tespiti üzerine çalışma yapılmıştır. Bu çalışmada Root-MUSIC,ESPRIT algoritmalarının düşük SNR performans testleri yapılmıştır. Ölçümlerde 3 farklı 10 derece aralıklı kaynakta 4 anten ve 200 örnekleme sayısıyla RMSE hatası üzerinden karşılaştırılmıştır. Bu karşılaştırmaya aynı parametre değerleriyle hesapladığımız GPS aldatma saldırısı senaryo sonuçları da eklenip Şekil 5.14'de gösterilmiştir. GPS aldatma saldırısı sonuçlarının normalize RMSE değerlerinin biraz daha yüksek olmasının nedeni [1]'dekinin yerine birbirine çok daha yakın açılı 8 kaynağın tespitinin yapılmasıdır. Sonuç olarak tez kapsamında bulunan gibi düşük SNR'da ESPRIT'i daha başarılı göstermiştir.



Şekil 5.14: SNR Değeri Etkisi Çalışması [1] ve GPS Aldatma Saldırısı Karşılaştırması Sonuçları

* [1] yayın sonuçları

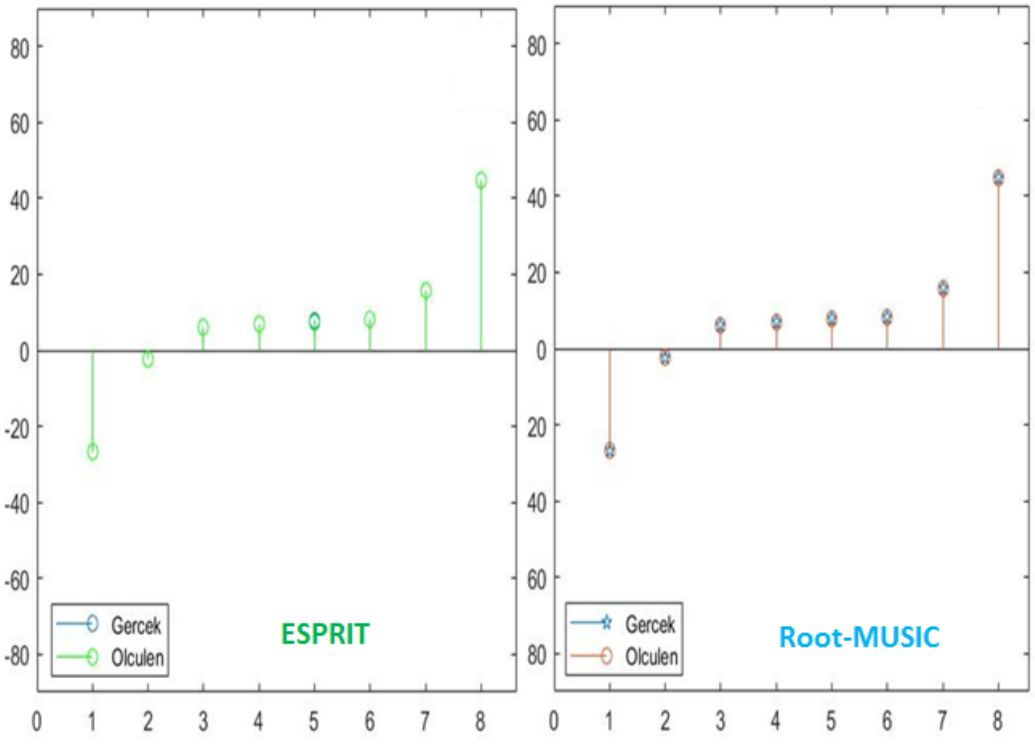
** GPS aldatma saldırı senaryosu sonuçları

5.7 Anten Dizi Mesafesi Farklılığında DOA Performansları

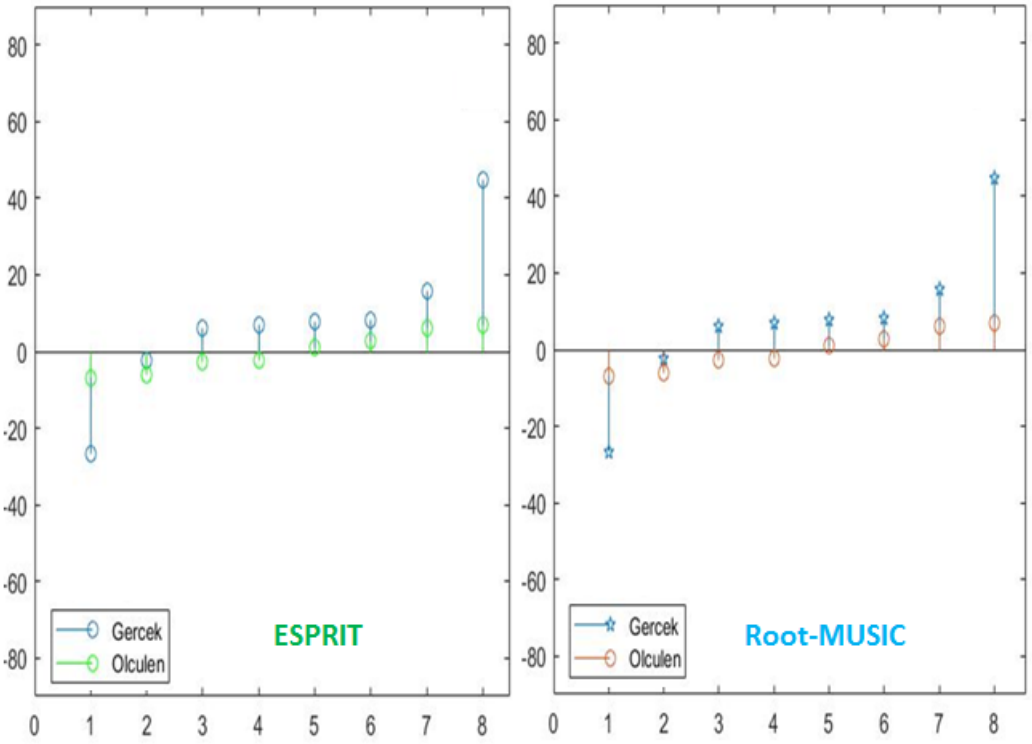
Anten dizilimleri ve aralarındaki mesafe diğer önemli bir değişken olduğundan tezin bu kısmında incelenmiştir. GPS aldatma saldırısı tespit uygulama biriminin oluşturulmasında anten sayısı ve anten dizisinin toplam boyutunu belirleyecektir. Bu durum çıkacak ürünün uygulanabilirliğini ortaya çıkaracaktır. SNR=50, Anten Sayısı=20 Örnek Sayısı=100 alınarak dizi aralığı λ dalga boyunda $\lambda/8$ ve 4λ arasında değiştirilerek sonuçlar Tablo 5.10'de karşılaştırılmıştır. Şekil 5.15'de $\lambda/2$ üzerinde Şekil 5.16 4λ üzerinden hesaplamalar gösterilmiştir.

Tablo 5.10: Anten Dizi Aralığı Değerleri Açısından ESPRIT ve Root-MUSIC Karşılaştırması

Anten Dizi Aralığı	ESPRIT (Toplam Hata)	Root-MUSIC (Toplam Hata)
$\lambda/8$	X	X
$\lambda/4$	1.1447	1.4329
$\lambda/2$	0.2955	0.1900
λ	61.8887	61.8891
4λ	100.8073	100.8073



Şekil 5.15: ESPRIT & Root-MUSIC $\lambda/2$ DOA Kestirimi



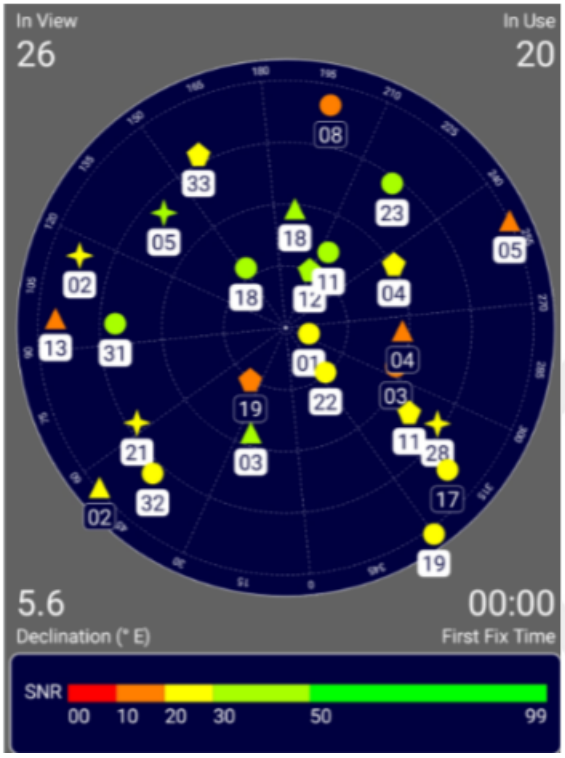
Şekil 5.16: ESPRIT & Root-MUSIC 4λ DOA Kestirimi

Burada gözlemlenen 2 algoritmanın anten aralığa gösterdiği tepki birbirine yakındır. En uygun anten aralığı dalga boyunun yarısı olan $\lambda/2$ olarak görülmüştür. Anten mesafesi kısaltıldığında dalga boyu kaçırılacağından dolayı belli aralıktan sonra hesaplama yapılamamaktadır. Aralık artığında da hata oranının arttığı ve ölçümlerinde gerçek değerden uzaklaştığı gözlemlenmiştir. [66] araştırmasında MUSIC ve ESPRIT algoritmalarını 0.15λ, 0.25λ, 0.5λ anten aralıklarıyla test edilmektedir ve en optimal olanı bizim de tespit ettiğimiz gibi 0.5λ bulunmuştur.

5.8 Saldırgan Kaynak Sayısı Farklılığında DOA Performansı

Bu karşılaştırmada çoklu kaynak sayısında değişimde algoritmaların performanslarına bakılacaktır. Türkiye'de aynı anda maksimum görülebilecek GPS uydu sayısı 10 adettir ama genelde 4-6 arası değişir. Çoklu GNSS alıcıları gibi diğer GNSS sistemlerinin de kullanıldığı yapılarda kompleks saldırı yapanlar diğer GNSS uydu sistemlerini de taklit etmesi gerekir. Şekil 5.17'da İstanbul Ataşehir'den çoklu GNSS alıcısı ile alınan kayıt

görüntüsü vardır. Burada GLONASS, GALILEO ve GPS sisteminin aktif olduğu ve aynı anda 26 uydudan veri alındığı gözlemlenmiştir.



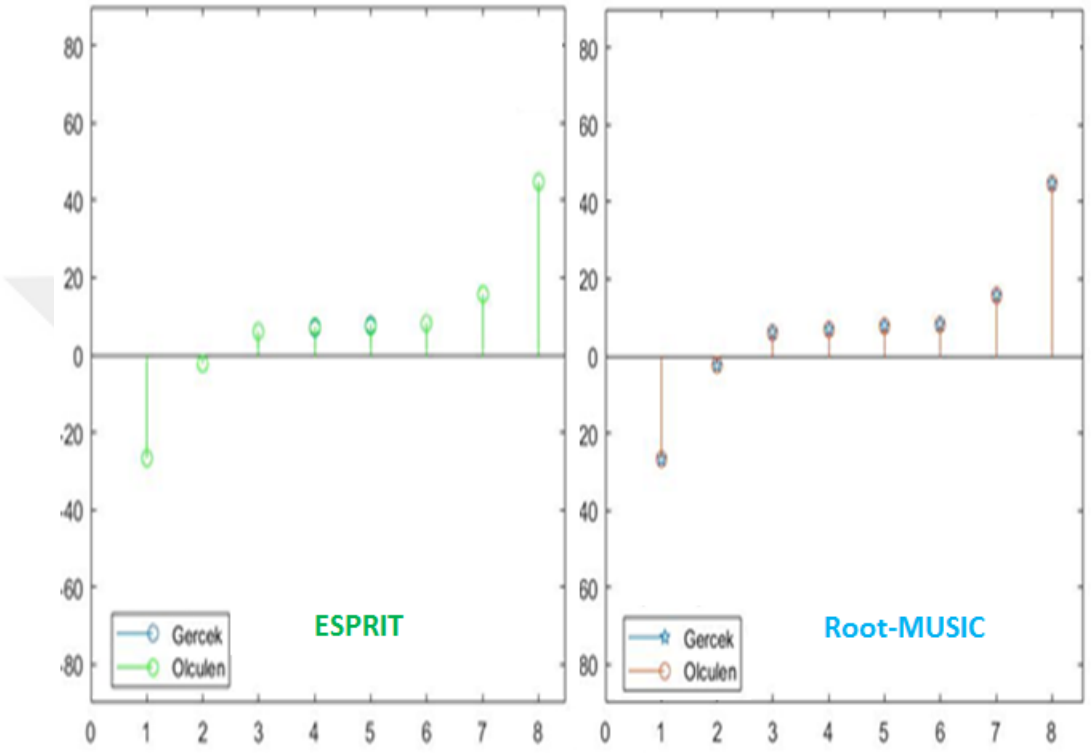
Şekil 5.17: Çoklu GNSS Alıcısı Uydu Haritası

Tablo 5.11: Saldırgan Kaynak Sayısına Göre DOA Performansları

Kaynak Sayısı	ESPRIT (Toplam Hata)	Root-MUSIC (Toplam Hata)
8	0.0012	0.00083484
10	0.0072	0.0069
12	0.0397	0.0106
14	0.6445	0.6264
16	70.425	30.2873
18	X	84.2139
20	X	115.7688

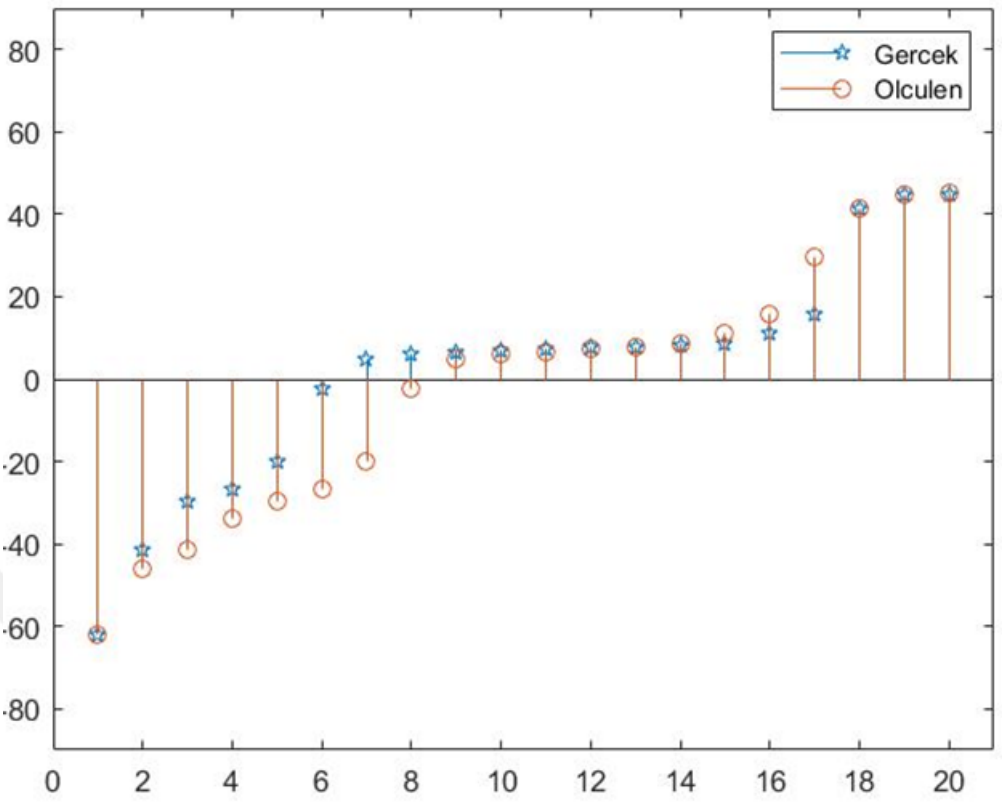
Çoklu GNSS alıcısı kullanıldığında kaynak sayısı artmaktadır ve bu karşılaştırmada kompleks (çoklu kaynaklı) GPS aldatma saldırılarına karşı tespit performansı Tablo 5.11'de gösterilmektedir. Uydu Sayısı=70, SNR=50, Örnek Sayısı=100 üzerinden hesap yapılmıştır. Uydu sinyal kaynakları ve GPS aldatma kaynakları toplamında bakılınca 8 - 20 arası kaynak üzerinden uydu sayısı, SNR ve örnek sayısı parametreleri sabit tutularak hesaplamalar yapılmıştır ve hata oranları kaynak sayısı arttıkça yükselmiştir. Bu nedenle kaynak sayısı farklılığındaki performansı görebilmek için anten sayısı ve örnek sayısı diğer

uygulamalara göre yüksek tutulmuştur. Şekil 5.18'de düşük kaynak sayısında gerçek ve hesaplanan açılar yüksek başarımda eşleşir ve üstüste gelmişlerdir; ancak kaynak sayısı artınca Şekil 5.19'deki gibi açı farkı artar.



Şekil 5.18: ESPRIT & Root-MUSIC 8 Kaynak DOA Kestirimi

Elde edilen bu sonuçlar doğrultusunda kaynak sayısı arttıkça Root-MUSIC performansının daha iyi olduğu ortaya çıkmıştır.

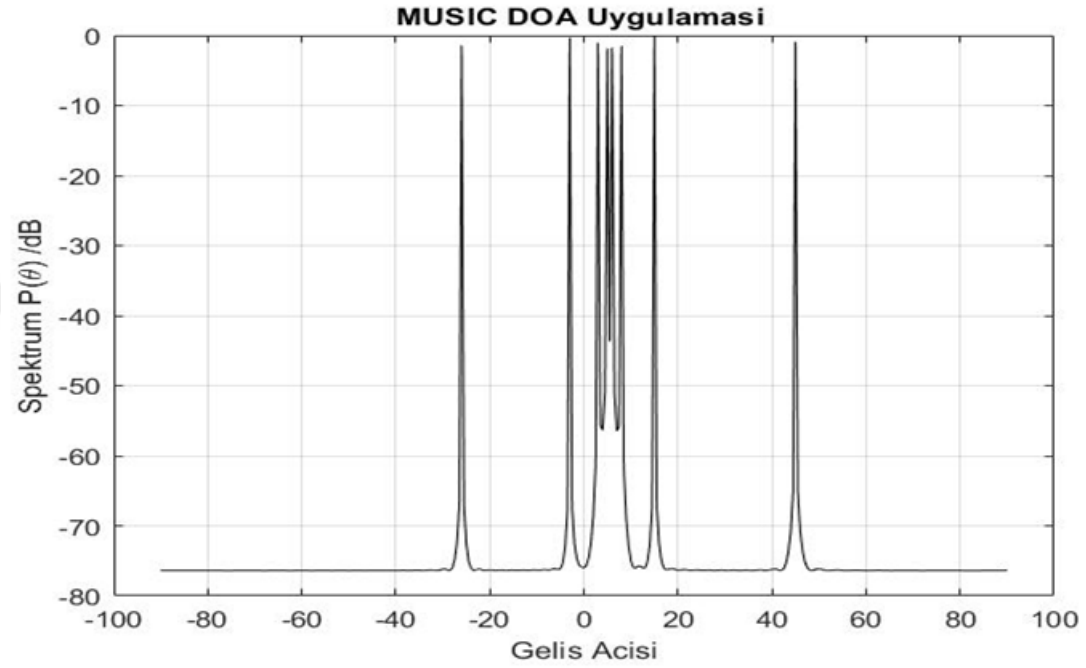


Şekil 5.19: Root-MUSIC 20 Kaynak DOA Kestirimi

5.9 MUSIC Algoritması DOA Performansı

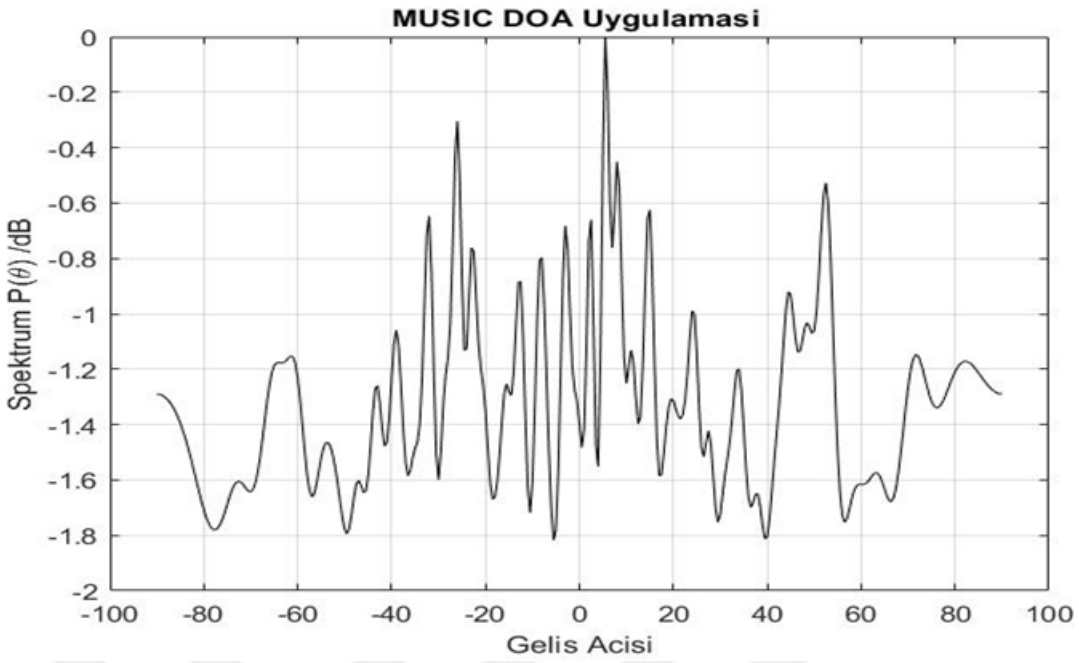
MUSIC algoritmasında GPS aldatma saldırısı tespiti oldukça zordur, normal DOA uygulamalarında MUSIC iyi sonuç vermektedir ama GPS sinyalleri aynı frekans bandında yayın yaptığı için MUSIC algoritması düzgün çalışmamaktadır. Bu sorunun dışında MUSIC algoritmasının temel sorunlarından biri de MUSIC algoritmasının tüm uzayı taramak zorunda olması nedeniyle getirdiği iş yüküdür. MUSIC kestirim başarımını yükseltmek için anten sayısı artıkça işlem yükü artacaktır ve komplekslik arttıkça algoritmanın kullanılabilirliği de azalır. MUSIC algoritmasının MATLAB uygulamasında farklı frekanslarda DOA tespiti yapıldığında Şekil 5.20 'deki gibi %1 altında hata ile başarmıştır .Şekil 5.20 'da her kaynağın açı değerleri belirgin olarak görülmektedir; ancak aynı frekansta test edildiğince DOA algoritması çalışmamıştır. Şekil 5.21 'deki aynı frekanstaki DOA hesaplaması gösterimde ise sinyal kaynağı tespiti yapılamamaktadır. [48] tezinde farklı algoritmalar, farklı parametrelerle karşılaştırılmıştır ve yaptığı çalışmalarda MUSIC algoritmasın aynı frekanslı yayınlarda açı tespitinin zorluğu, tüm uzayı taramak zorunda olmasının beraberinde getirmiş olduğu işlem yükü aynı şekilde gözlemlenmiştir. Anten

sayısı ve örnek sayısının artması algoritmaların çalışmasını zorlar, işlem yükü artar ve hesaplama uzun süreler alır. Bu kriterler dikkate alındığında MUSIC,Root-MUSIC ve ESPRIT'e göre çok geride kalır.

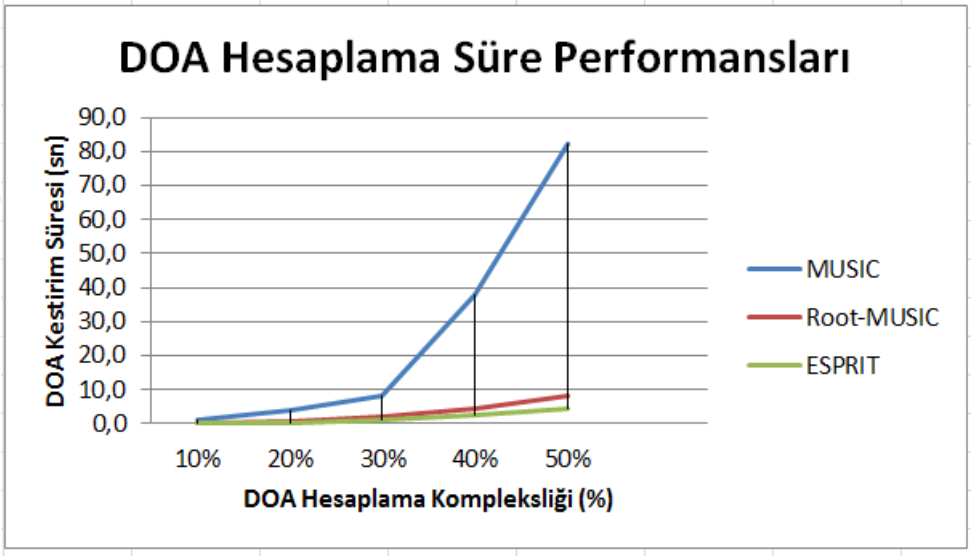


Şekil 5.20: Farklı Frekanslarda MUSIC DOA Performansı

DOA hesaplama hızlarını karşılaştırmak için MATLAB uygulamasın DOA hesaplama kompleksliği anten sayısı, örnek sayısı gibi parametreleri sırasıyla arttırılarak ayarlanır. Intel Core i7 3610 QM,2.3GHz 8GB RAM donanımı ve %100'e yakın CPU ile çalıştığında elde edilen hesaplama süresi verileri Şekil 5.22 'deki gibidir ve bu sonuçlara göre ESPRIT diğer algoritmalara göre hız bakımından daha başarılıdır.



Şekil 5.21: Aynı Frekanslarla MUSIC DOA Performansı

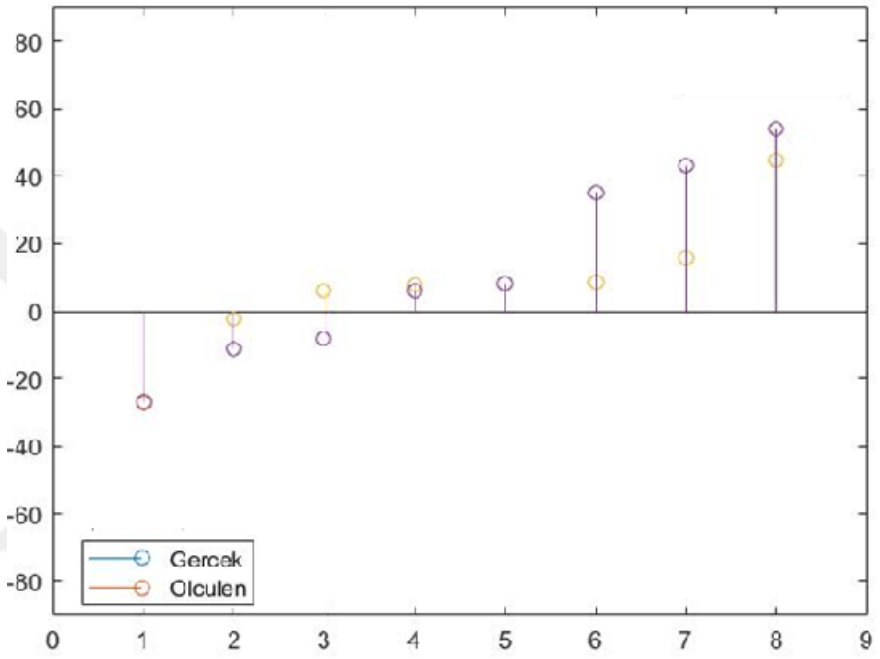


Şekil 5.22: DOA Performans Karşılaştırması

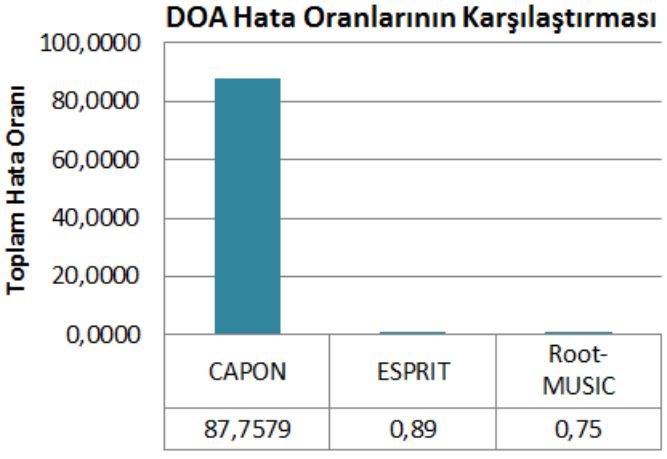
5.10 CAPON Algoritması DOA Performansı

CAPON, Root-MUSIC ve ESPRIT algoritmasına göre çok daha verimsiz bir algoritmadır; özellikle GPS aldatma saldırısında aynı bölgede tek kaynak olduğundan birbirine yakın kaynakları tespit etmek çok zordur. Bu nedenle ESPRIT ve Root-MUSIC ile parametre karşılaştırmalarına katılmamıştır. CAPON ile diğer algoritmaları karşılaştırmak için yüksek çözünürlük hesabı beklediğimiz Örnek Sayısı:200, Uydu Sayısı :50, SNR:40

parametre değerleri olacak şekilde uygulamaya konulduğunda 87.7579 derecelik hata değeriyle DOA açıları bulunur. ESPRIT ve MUSIC %1 in çok altında hata ile yönleri tespit edebilmiştir. Bu karşılaştırma verileriyle de CAPON'un düşük başarımı ortaya konmuştur. Şekil 5.23'de gerçek ve ölçülen kaynak açılarının arasında farkların sonuçlar gösterilmiştir. DOA algoritmalarının arasındaki fark ise Şekil 5.24'de gösterilmiştir.



Şekil 5.23: CAPON DOA Düşük Performansı Gösterimi



Şekil 5.24: DOA Hata Oranları Karşılaştırması

Bölüm 6

Sonuçlar

Bu tez çalışması ile DOA algoritmalarının GPS saldırılarının tespitinde kullanılabilirliği gösterildi ve yeni gelişen karmaşık saldırı senaryolarına karşı parametre optimizasyonları yapılarak mevcut çözümlerin başarımı artırıldı. Bu başarıma ulaşabilmek için öncelikle GPS sisteminin tanıtımı, çalışma yapısı, sistem bileşenleri anlatıldı. GPS sisteminin güvenliği üzerine yapılan anlatımda sistem güvenlik gerekleri ve mevcut sistem açıklıklarından bahsedildi. Bu açıklıklar doğrultusunda yapılan GPS aldatma ve GPS sinyal karıştırma saldırıları, bu saldırıların tespiti ve önlemine yönelik incelemeler yapıldı. GPS sistemine yapılan saldırıların tespiti ve önlenmesi için yapılanlar sensör ve harici doğrulama referanslarının kullanımı, GPS alıcı ve anten kısmında alınan tedbirler başlıklarıyla ele alınıp karşılaştırmalı olarak anlatıldı.Hem GPS aldatma saldırısında hem de sinyal karıştırma saldırısında kullanılabilir olmasından ve kompleks GPS aldatma saldırıların tespitindeki başarısından dolayı tez kapsamındaki uygulamalarda GPS saldırı tespit metodu olarak DOA kullanılmıştır.

DOA tespit algoritmaları üzerine yaptığımız çalışmada ise SNR değerinin, örnek sayısının ve anten sayısının DOA tespitinde etkili olduğu gözlemlenmiştir. MUSIC algoritması hem tüm uzayı taramak zorunda olması nedeniyle çok iş yükü vardır hem de aynı frekanslı sinyallerde yön tespiti başarısızdır. CAPON algoritmasın temeli tek kaynaklı sinyal tespitine dayandığından Root-MUSIC ve ESPRIT algoritmalarına göre GPS aldatma saldırısı tespitinde çok başarısızdır. Bu nedenle karşılaştırmalar ESPRIT ve Root-MUSIC

arasında yapıldı. GPS sinyali düşük SNR değerine sahip olduğunda ESPRIT bu özellikle daha başarılıdır; ancak sinyal seviyesi güçlendikçe iki algoritma da çok iyi performans göstermektedir. Düşük anten sayısında da düşük örnek sayısında da ESPRIT Root-MUSIC algoritmasına göre daha başarılıdır. Bunun temel nedeni ESPRIT algoritmasının GPS aldatma saldırılarındaki gibi yakın açılı kaynakların tespitinde daha başarılı olmasıdır.Tablo 6.1'de MATLAB DOA saldırı simülasyonlarının sonucu olarak elde edilen değerlerin karşılaştırması vardır. Karşılaştırma çözünürlük hassasiyeti üzerinden yapılır. Toplam açı hata değerlerinin karşılaştırıldığı bu tabloda sonuçlara ulaşabilmek için diğer parametreler sabit tutulup karşılaştırılacak parametrelerde değişiklikler yapılmıştır. Tüm hesaplamalar aynı işleme yeteneğine sahip donanım üzerinde parametre değişiklikleri yapılarak yapılmıştır. Belirlenen hata eşik değerlerine göre "Çok İyi"den "Kötü"ye göre sonuçlar sıralanmıştır.

Tablo 6.1: MATLAB DOA Uygulaması Performans Karşılaştırması

DOA Algoritması	ESPRIT	Root-MUSIC	MUSIC	CAPON
Düşük Örnekleme Sayısı	İyi	Orta	Kötü	Kötü
Yüksek Örnekleme Sayısı	Çok İyi	Çok İyi	Orta	Orta
Düşük SNR Seviyesi	Orta	Kötü	Kötü	Kötü
Yüksek SNR Seviyesi	Çok İyi	Çok İyi	Orta	Orta
Düşük Anten Sayısı	Orta	Kötü	Kötü	Kötü
Yüksek Anten Sayısı	Çok İyi	Çok İyi	Orta	Orta
Yakın Açı	Çok İyi	Çok İyi	Orta	Kötü
Uygulanabilirlik	Çok İyi	Çok İyi	Kötü	Orta
Çok kaynaklı Saldırı	Çok İyi	Çok İyi	Orta	Kötü

GPS sinyal karakteristik özellikleri ve karmaşık saldırı teknikleri dikkate alınarak GPS aldatma saldırısının tespitinde yüksek çözünürlükte başarım elde edilmesi için düşük SNR değerinde, çoklu kaynaklı saldırılarda, hızlı işlem süreleriyle yüksek başarımda tespit hedeflenmektedir. Bu durumda yüksek örnekleme, yüksek anten sayısı, λ /2 anten aralığı ile ESPRIT algoritmasının kullanılması gerekmektedir.

Gelecek çalışmalarda bu parametre optimizasyonunun saldırı boyutuna ve türüne göre yapay zeka ya da adaptif algoritmalarla ayarlanan sistemlerin geliştirilmesi olabilir.

Kaynakça

[1] N. Anwar and B. M. Mohammad. Comparison of direction of arrival (doa) estimation techniques for closely spaced targets. *International Journal of Future Computer and Communication*, pages 654–659, 01 2013.

[2] M. V. Madhava. A comparative study of doa estimation algorithms with application to tracking using kalman filter. *Signal Image Processing : An International Journal*, 6:13–29, 12 2015.

[3] *GPS Standard Positioning Service (SPS) Performance Standard, US Department of Defence*. US Department of Defence, Washington, D.C, 4nd edition, 2008.

[4] Why was loran such a milestone?, 2018. URL `https://timeandnavigation.si.edu/navigating-air/navigation-at-war/new-era-in-time-and-navigation/loran`.

[5] Loran-long range navigation basics, 2016. URL `http://www.rfwireless-world.com/Terminology/LORAN-Long-Range-Navigation.html`.

[6] B. H.Wellenhof, H. Lichtenegger, and E. Wasle. *GNSS Global Navigation Satellite Systems: GPS, GLONASS, Galileo, and more*. Springer Wien, New York, 2008.

[7] Gnss (global navigation satellite systems), 2017. URL `https://spotlight.unavco.org/how-gps-works/gps-basics/gnss-global-navigation-satellite-systems.html`.

[8] The downing of flight 007: 30 years later, a cold war tragedy still seems surreal, 2013. URL `https://edition.cnn.com/2013/08/31/us/kal-fight-007-anniversary/index.html`.

[9] Global positioning system, 2017. URL `https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS.html`.

[10] Augmentation systems, 2018. URL `https://www.gps.gov/systems/augmentations/`.

[11] Nokta konumları, 2018. URL `https://www.tkgm.gov.tr/tr/noktakonumlar%C4%B1`.

[12] G. Djuknic and R. Richton. Geolocation and assisted gps. *IEEE Computer*, 34: 123–125, 03 2001.

[13] Fcc to vote to allow u.s. devices to use european navigation system, 2018. URL `https://www.reuters.com/article/us-usa-fcc-gps-europe/fcc-to-vote-to-allow-u-s-devices-to-use-european-navigation-system`.

[14] The gps, 2016. URL `http://www.math.tamu.edu/~dallen/physics/gps/gps.htm`.

[15] O. S. Heon, S. Lee, C. Park, and D. Hwang. Design of a low-cost attitude determination gps/ins integrated navigation system for a uav (unmanned aerial vehicle). *Journal of Institute of Control, Robotics and Systems*, 01 2005.

[16] *Global Positioning Systems Standard Positining Service Signal Specifications*. US Department of Defence, Washington, D.C, 2nd edition, 1995.

[17] Gps at schriever, 2017. URL `https://www.schriever.af.mil/GPS/`.

[18] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun. On the requirements for successful gps spoofing attacks. In *ACM Conference on Computer and Communications Security*, 2011.

[19] J. Nielson, J. Keefer, and B. McCullough. Saasm: Rockwell collins' next generation gps receiver design. In *IEEE 2000. Position Location and Navigation Symposium (Cat. No.00CH37062)*, pages 98–105, March 2000. doi: 10.1109/PLANS.2000.838289.

[20] Over-the-air distribution (otad) update, 2015. URL `https://www.gps.gov/multimedia/presentations/2015/04/partnership/tyley.pdf`.

[21] Iran unveils new ucav modeled on captured u.s. rq-170 stealth drone, 2016. URL `https://theaviationist.com/2016/10/02/iran-unveils-new-ucav-modeled-on-captured-u-s-rq-170-stealth-drone/`.

[22] Finland summons russia ambassador over jammed gps during nato drills, 2018. URL https://www.euronews.com/2018/11/17/finland-summons-russia-ambassador-over-jammed-gps-during-nato-drills.

[23] Ships fooled in gps spoofing attack suggest russian cyberweapon, 2013. URL https://www.ainonline.com/aviation-news/aviation-international-news/2013-08-02/south-korea-install-eloran-counter-north-korean-gps-jamming.

[24] Car jammers: Interference analysis, 2011. URL https://www.gpsworld.com/transportationroadcar-jammers-interference-analysis-12128/.

[25] O. Glomsvoll and L. K. Bonenberg. Gnss jamming resilience for close to shore navigation in the northern sea. *Journal of Navigation*, 70(1):33â48, 2017.

[26] The role of gnss antennas in mitigating jamming and interference, 2009. URL https://www.u-blox.com/sites/default/files/products/documents/u-blox-AntiJamming_WhitePaper_%28GPS-X-09008%29.pdf.

[27] Anti-jamming techniques in u-blox gps receivers, 2012. URL http://insidegnss.com/pdf/Inside_GNSS_12.05.13_GNSS_antennas_webinar_slides.pdf.

[28] 16-channel gps constellation simulator, 2011. URL http://gpsworld.com/professional-oem16-channel-gps-constellation-simulator-11178/.

[29] D. A. Schmidt, K. Radke, S. A. Çamtepe, E. Foo, and M. Ren. A survey and analysis of the gnss spoofing threat and countermeasures. *ACM Comput. Surv.*, 48: 64:1–64:36, 2016.

[30] S. Seo, B. Lee, S. Im, and G. Jee. Effect of spoofing on unmanned aerial vehicle using counterfeited gps signal. *Journal of Positioning, Navigation, and Timing*, 4: 57–65, 06 2015.

[31] A. Ranganathan, H. Ölafsdöttir, and S. Capkun. Spree: a spoofing resistant gps receiver. In *MobiCom*, 2016.

[32] Bluesky gnss firewall, 2019. URL https://www.microsemi.com/product-directory/gps-instruments/4398-bluesky-gps-firewall.

[33] Inertial navigation systems (ins) explained, 2015. URL `https://www.oxts.com/what-is-inertial-navigation-guide/`.

[34] S. Khanafseh, N. Roshan, S.Langel, F. C. Chan, M. Joerger, and B. Pervan. Gps spoofing detection using raim with ins coupling. *Proceedings of IEEE/ION PLANS 2014*, 5:1232–1239, 05 2014.

[35] S. Riisgaard and M. R. Blas. Slam for dummies: A tutorial approach to simultaneous localization and mapping. Technical report, 2005. URL `http://ocw.mit.edu/courses/aeronautics-and-astronautics/16-412j-cognitive-robotics-spring-2005/projects/1aslam_blas_repo.pdf`.

[36] Urban mapping for autonomous car with slam, 2016. URL `https://kmatrix.kaist.ac.kr/urban-mapping-for-autonomous-car-with-slam/`.

[37] Guidelines for real-time kinematic (rtk) surveying, 2015. URL `https://canadiangis.com/guidelines-for-real-time-kinematic-rtk-surveying.php`.

[38] Current operational status of leo-satellite-based time and location, 2016. URL `https://www.gps.gov/governance/advisory/meetings/2018-05/gutt.pdf`.

[39] C. Yoo and I. Ahn. Low cost gps/ins sensor fusion system for uav navigation. In *Digital Avionics Systems Conference, 2003. DASC '03. The 22nd*, volume 2, pages 8.A.1–8.1–9 vol.2, Oct 2003.

[40] Gps-lidar fusion with 3d city models, 2017. URL `https://www.gpsworld.com/gps-lidar-fusion-with-3d-city-models/`.

[41] L. Xiao, P. C. Ma, X. M. Tang, and G. F. Sun. *GNSS Receiver Anti-spoofing Techniques: A Review and Future Prospects*, volume 382, pages 59–68. 01 2016.

[42] A. Hussain. *Electronics, Communications and Networks V: Proceedings of the 5th International Conference on Electronics, Communications and Networks (CECNet 2015)*, volume 382. 01 2016.

[43] Compact high-sensitive gps speedometer lc-8300, 2018. URL `https://www.onosokki.co.jp/English/hp_e/products/keisoku/automotive/lc8300.html`.

[44] Q. S. Ullah and A. Dempster. Cross-correlation performance comparison of l1 l2c gps codes for weak signal acquisition. 01 2008.

[45] L. Chiarello. Security evaluation of gnss signal quality monitoring techniques against optimal spoofing attacks. Master's thesis, Universita degli Studi di Padova, Padova,, Italy, 2018.

[46] Z. Chen, G. Gokeda, and Y.Yu. *Introduction to Direction of Arrival Estimation.* Artech House, Boston, D.C, 2010.

[47] T. E. Tuncer and B. Friedlander. *Classical and Modern Direction-of-Arrival Estimation.* Elsevier, Burlington, USA, 2009.

[48] S. Ö. Ata. Bir polar grid anten dizisiyle doa kestirimi. Master's thesis, İstanbul Teknik Üniversitesi, İstanbul, Türkiye, 2010.

[49] T. Dhope. Application of music, esprit and root music in doa estimation. 06 2019.

[50] G. K. Gokeda. Performance analysis of esprit based algorithms for doa estimation. Master's thesis, Dalhousie University, Virginia, USA, 2002.

[51] R. Sanudin, N. H. Noordin, A. O. El-Rayis, N. Haridas, A. T. Erdogan, and T. Arslan. Capon-like doa estimation algorithm for directional antenna arrays. In *2011 Loughborough Antennas Propagation Conference*, pages 1–4, Nov 2011.

[52] N. A. Baig and A. Hussain. Radar signal processing for target range, doppler and doa estimation. In *2017 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pages 820–825, Jan 2017.

[53] Ennas and propagation, 2015. URL `http://www.faculty.jacobs-university.de/jwallace/xwallace/courses/ap/ch5c.pdf`.

[54] C.A. Balanis. *Advanced Engineering Electromagnetics.* John Wiley Sons, 1989.

[55] C.A. Balanis. *Antenna Theory: Analysis and Design.* Wiley, River Street, New Jersey, USA, 1997.

[56] *NAVSTAR GPS User Equipment Introduction Navigation.* US Department of Homeland Security, Washington, D.C, center public edition edition, 1996.

[57] K. Wesson and T. Humphreys. Hacking drones. *Scientific American*, 309(5):54–59, 11 2013.

[58] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner. Assessing the spoofing threat: Development of a portable gps civilian spoofer. In *21st International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS 2008*, volume 2, pages 1198–1209, 12 2008.

[59] D. Borio, J. F. Guasch, and C. O'Driscoll. Spectral and spatial characterization of gnss jammers. 04 2013.

[60] L. Xiao, P. C. Ma, X. M. Tang, and G. F. Sun. *GNSS Receiver Anti-spoofing Techniques: A Review and Future Prospects*, volume 382, pages 59–68. 01 2016.

[61] T. B. Lavate, V. K. Kokate, and A. M. Sapkal. Performance analysis of music and esprit doa estimation algorithms for adaptive array smart antenna in mobile communication. *2010 Second International Conference on Computer and Network Technology*, pages 308–311, 2010.

[62] T. Orul. Akıllı anten sistemleri İçin İşaret geliş açısı kestirim yöntemleri. Master's thesis, Gazi Üniversitesi, Ankara, Türkiye, 2012.

[63] M. Meurer, A. Konovaltsev, M. Appel, and M. Cuntz. Direction-of-arrival assisted sequential spoofing detection and mitigation. 2016.

[64] Y. H. Chen, S. Lo, A. Perkins, F. Rothmaier, D. M. Akos, and P. Enge. Demonstrating single element null steering antenna direction finding for interference detection. 2018.

[65] S. Fortunati, R. Grasso, F. Gini, M. Greco, and K. Lepage. Single-snapshot doa estimation by using compressed sensing (jasp). *EURASIP Journal on Advances in Signal Processing*, 2014, 11 2014.

[66] B. N. Bansode and N. A. Dheringe. Performance evaluation and analysis of direction of arrival estimation using music, tls esprit and pro esprit algorithms. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 04:4948–4958, 06 2015.