GNSS ALDATMA KARŞITI BİR ALMAÇ MİMARİSİNİN GELİŞTİRİLMESİ

DEVELOPMENT OF A GNSS ANTI SPOOFING RECEIVER ARCHITECTURE

MELİH TİMURCAN KURALAY

DR. ÖĞR. ÜYESİ YAKUP ÖZKAZANÇ

Tez Danışmanı

Hacettepe Üniversitesi

Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin

Elektrik ve Elektronik Mühendisliği Anabilim Dalı için Öngördüğü

YÜKSEK LİSANS TEZİ olarak hazırlanmıştır.

2024

ÖZET

GNSS ALDATMA KARŞITI BİR ALMAÇ MİMARİSİNİN GELİŞTİRİLMESİ

Melih Timurcan KURALAY

Yüksek Lisans, Elektrik ve Elektronik Mühendisliği Bölümü

Tez Danışmanı: Dr. Öğr. Üyesi Yakup Özkazanç

Eylül 2024, 83 sayfa

GNSS aldatma saldırıları, uydu sinyallerini taklit ederek GNSS alıcısını aldatmak ve olmadığı bir konumdaymış gibi göstermek için yapılan saldırılardır ve havacılık, askeri operasyonlar ve otonom araçlar gibi kritik uygulamalarda kullanılan GNSS alıcıların güvenliğini tehdit eder. Bu saldırılar günümüzde radyo frekans modüllerinin yaygınlaşması ile beraber hızla gelişmiştir. Bu durum, aldatma saldırılarının artmasına neden olurken, aynı zamanda aldatma karşıtı tedbirlerin geliştirilmesi elzem hale gelmiştir. Aldatma karşıtı önlemler ise bu aldatma saldırılarını bertaraf etmek için alıcılara entegre edilen özelliklerdir ve aldatma karşıtı almaç mimarisi de bu tür tehditleri etkili bir şekilde tespit etmek ve azaltmak için çeşitli tekniklerin ve yöntemlerin alıcılara entegre edilmesini kapsar.

Bu çalışma kapsamında, literatürde bulunan aldatma saldırıları kapsamlı bir şekilde incelenmiştir. Farklı türdeki aldatma saldırıları, bu saldırıların temel mekanizmaları ve çeşitli sistemler üzerindeki potansiyel sonuçları sistematik bir şekilde anlatılmıştır. Bu saldırıların etkileri, karmaşıklık seviyeleri ve tespit edilip engellenmesinde karşılaşılan zorluklar, ayrıntılı bir şekilde sistematik olarak anlatılmıştır. Bu anlatımlar, çeşitli aldatma tekniklerinin oluşturduğu tehditlerin ciddiyetini, bunların tespit edilmesi ve hafifletilmesi sürecindeki karmaşıklıkları vurgulamak amacı taşımaktadır.

Ayrıca, bu saldırılara karşı uygulanan çeşitli aldatma karşıtı yöntemler de incelenmiştir. Her yöntem, etkinliği açısından eleştirel bir şekilde değerlendirilmiş ve hangi senaryolarda en etkili veya en az etkili olduklarına dikkat edilmiştir. Bir dizi deneysel çalışma yoluyla, mevcut aldatma karşıtı tedbirlerin belirli zayıflıkları ve sınırlamaları tespit edilmiştir. Bu zayıflıklar dikkatlice analiz edilerek, bu açıkların nedenleri ve potansiyel riskleri anlatılmıştır.

Bu analizlerden elde edilen bulgulara dayanarak, mevcut önlemlerin eksikliklerini gidermeyi hedefleyen yeni ve güvenilir bir aldatma karşıtı mimari önerilmiştir. Önerilen bu mimari, yalnızca bilinen aldatmaya açık kısımları hafifletmekle kalmayıp, aynı zamanda ortaya çıkan tehditlere yanıt verebilecek daha uyarlanabilir ve dirençli bir savunma mekanizması sunmayı amaçlamaktadır. Önerilen çözüm, pratik uygulamalarda uygulanabilirliği ve etkinliği açısından kapsamlı bir şekilde değerlendirilmiş olup, güvenliği artırma çabalarına önemli bir katkı sağlamaktadır.

Anahtar Kelimeler: GPS, GNSS, GNSS aldatma, GNSS aldatma karşıtı tedbirler, CRPA anten, INS/IMU sensörler

ABSTRACT

DEVELOPMENT OF A GNSS ANTI SPOOFING RECEIVER ARCHITECTURE

Melih Timurcan KURALAY

Master of Science, Department of Electrical and Electronics Engineering

Supervisor: Assist. Prof. Dr. Yakup Özkazanç

September 2024, 83 pages

GNSS spoofing attacks are conducted to deceive a GNSS receiver by imitating satellite signals, making it appear to be at a different location than it actually is. These attacks threaten the security of GNSS receivers used in critical applications such as aviation, military operations, and autonomous vehicles, and, consequently, the security of these applications. With the proliferation of radio frequency modules, these attacks have rapidly advanced, making the development of anti-spoofing measures essential. Anti-spoofing measures are features added to receivers to counter these spoofing attacks, and an anti-spoofing receiver architecture involves integrating various techniques and methods into receivers to effectively detect and mitigate such threats.

In this study, spoofing attacks found in the literature were comprehensively examined. Different types of spoofing attacks, their underlying mechanisms, and their potential impacts on various systems were systematically described. The effects of these attacks, their complexity levels, and the challenges encountered in detecting and preventing them have been systematically described in detail. These descriptions aim to emphasize the severity of the threats posed by various spoofing

techniques and the complexities involved in their detection and mitigation processes.

Additionally, various anti-spoofing methods applied against these attacks were also examined. Each method was critically evaluated in terms of its effectiveness, with attention given to the scenarios in which they are most and least effective. Through a series of experimental studies, specific weaknesses and limitations of the existing anti-spoofing measures were identified. These weaknesses were carefully analyzed to explain their causes and potential risks.

Based on the findings from these analyses, a new and reliable anti-spoofing architecture was proposed to address the shortcomings of current measures. This proposed architecture aims not only to mitigate known vulnerabilities but also to offer a more adaptable and resilient defense mechanism capable of responding to emerging threats. The proposed solution was thoroughly evaluated for its practicality and effectiveness in real-world applications, making a significant contribution to efforts to enhance security.

Keywords: GNSS, GPS, GNSS spoofing, GNSS anti-spoofing, CRPA antenna, INS/IMU sensors

TEŞEKKÜR

Yüksek lisans eğitimim boyunca, hiçbir konuda desteğini esirgemeyen, engin bilgi birikimi ve geniş vizyonu ile her zaman yol göstericim olan değerli danışmanım Sayın Dr. Öğr. Üyesi Yakup Özkazanç'a,

Her zaman koşulsuz desteğini hissettiğim babam Telat KURALAY, annem Nergiz KURALAY ve abim Enver Kaan KURALAY'a,

Yüksek Lisans sürecinin en başından beri bana destek sağlayan ve araştırmalarımda gerekli kaynakları sunan DEICO Mühendislik A.Ş.'ye,

DEICO Mühendislik A.Ş.'de birlikte çalıştığım tüm mesai arkadaşlarıma verdikleri destekten dolayı,

Teşekkürlerimi sunarım.

Melih Timurcan KURALAY

Eylül 2024, Ankara

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

SİMGELER VE KISALTMALAR

Simgeler

c	Işık hızı
σ	Standart Sapma
μ	Aritmetik ortalama
ζ	Sönüm oranı
°	Derece
W	Watt
P	Güç

Kısaltmalar

A/S	Anti Spoofing
ABD	Amerika Birleşik Devletleri
ADC	Analog to Digital Converter
ANS	Ataletsel Navigasyon Sistemi
BPF	Band Pass Filter
BOC	Binary Offset Carrier
C/A	Clear Acquisition - Coarse Acquisition
CMDA	Code Division Multiple Access
CNAV	Civil Navigation
DOF	Degrees of Freedom
DOP	Dilution of Precision
DC	Direct Current
ECEF	Earth-Center, Earth-Fixed
FDMA	Frequency Division Multiple Access

FEA	Forward Estimaton Attack
FLL	Frequency Locked Loop
FPGA	Field Programmable Gate Array
GMT	Greenwich Mean Time
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GRC	GNU Radio Companion
IEEE	Institute of Electrical and Electronics Engineers
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
ITRF	International Terrestrial Reference Frame
KUSS	Küresel Uydu Seyrüsefer Sistemi
LHCP	Left-Handed Circularly Polarized
LNAV	Legacy Navigation
LNA	Low Noise Amplifier
MCS	Master Control Station
NAV-PVT	Navigation Position Velocity Time
NMEA	National Marine Electronics Association
NTP	Network Time Protocol
P Code	Precise/ Protected Code
PRN	Pseudo Random Code
PLL	Phase Locked Loop
RF	Radio Frequency
RHCP	Right-Handed Circularly Polarized
RINEX	Receiver Independent Exchange
RTCM	Radio Technical Commission for Maritime Services

RTK	Real Time Kinematic
SA	Selective Availability
SAASM	Selective Availability Anti-Spoofing Module
SAW	Surface Acoustic Wavex
SCER	Security Code Estimation and replay
SDR	Software Defined Radio
SPS	Standard Positioning Service
SV	Satellite Vehicle
USB	Universal Serial Bus
USRP	Universal Software Radio Peripheral
UTC	Coordinated Universal Time
UTM	Universal Transverse Mercator
NAV-TP	Navigation Time Pulse

SÖZLÜK DİZİNİ

İNGİLİZCE	TÜRKÇE
3D - Fix	3D Konum Sabitleme
Carrier	Taşıyıcı
Frequency Locked Loop (FLL)	Frekans Kenetleme Döngüsü
Gain	Kazanç
GNSS	Küresel Seyrüsefer Uydu Sistemi
In-phase	Eşevreli
Modulation	Kiplenim
Multipath	Çokyolluluk
Navigation	Navigasyon, Seyrüsefer
No-fix	GNSS sabitlenememesi
Noise Figure	Gürültü katsayısı
Phase Locked Loop (PLL)	Evre Kenetleme Döngüsü
Precise Positioning Service (PPS)	Hassas Konumlandırma Servisi
Pseudo Random Noise	Sözde Rastlantısal Gürültü
Pseudorange	Sözde Mesafe

1. GİRİŞ

Günümüzde küresel seyrüsefer uydu sistemleri (GNSS) sivil ve askeri operasyonlar için kritik öneme sahip olan navigasyon, zamanlama ve konum hizmetleri gibi birçok uygulamanın temelini oluşturmaktadır. Bu sistemlerin uygulama alanları gün geçtikçe artmakta ve bu sistemler teknolojik altyapımızda giderek daha kritik roller oynayacaktır. Bu yüzden GNSS alıcılarını yanıltan sahte sinyallerin kullanıldığı aldatma saldırıların oluşturduğu güvenlik tehditleri önemli bir endişe haline gelmiştir. Aldatma saldırısı, GNSS alıcılarını aldatmak için sahte sinyaller yaymakla beraber sadece GNSS alıcılarını aldatmakla kalmayıp havacılık, deniz navigasyonu, otonom araç güdümü, füze sistemleri gibi GNSS verilerinin güvenirliğine dayanan sistemleri tehlikeye atar [1]. Bu yüzden günümüzde birçok sektörde kullanılan GNSS sistemlerinin bir saldırı karşısında dayanıklı olması bir iyileştirmeden öte zorunluluk haline gelmiştir.

GNSS sistemlerin aldatma saldırılarına karşı savunmasızlığı ile ilgili ilk endişeler 1990'larda ortaya çıkmıştır. Bu yıllarda GNSS sinyallerinin kolay bir şekilde kopyalanabileceğini vurgulayan ilk araştırmalar ve bazı gösterimler yapıldı. Buna karşılık ABD ordusu o yıllarda seçici erişilebilirlik sahteciliği önleme modülü (SAASM) gibi uydudan şifreli bir sinyal yayılımı yapıp bu şifreli sinyali çözebilen bir modül kullanmaya başlamıştır. Ardından yüksek profilli bir gösterim olarak geçen ve 2013 yılında sahte GPS sinyalleri kullanarak bir yatın navigasyon sisteminin kontrolünü ele geçirmeyi başaran Texas Üniversitesi araştırmacıları sayesinde, 2010'larda halkın farkındalığı önemli ölçüde arttı. Ayrıca Kırım ve Suriye gibi çatışma bölgelerinde GNSS aldatma yapıldığına ilişkin raporlar, jeopolitik sonuçların ve deniz ve hava güvenliği üzerindeki etkisinin önemini artırdı [2].

Aldatma saldırılarının yarattığı güvenlik zafiyetleriyle mücadele etmek için bu tehditleri tesbit edebilen, aldatma saldırısına karşı dayanıklı GNSS alıcı mimarisinin geliştirilmesi hayati önem taşımaktadır. Aldatma saldırılarına karşı geliştirilen mimariler genellikle GNSS sinyallerinin alınmasında güvenirliği ve doğruluğu sağlayarak aldatma saldırılarını tespit etmek ve hafifletmek üzerine alınan tedbirlerdir. Aldatma karşıtı teknolojiler aslında basit veya karmaşık bir şekilde GNSS alıcılarına yapılan aldatma saldırılarını bertaraf etmek için sahte ve gerçek GNSS sinyallerini ayırt edebilen ileri seviyede algoritmalar ve donanım iyileştirmeleridir. Bu sayede sistemlerin kritik karar verme süreçlerinde kullanılan

verilerin bütünlüğünü korur. Bu çalışmada ileri düzey GNSS aldatma karşıtı bir alıcının mimarisinde bulunabilecek bileşenler ve çalışma prensipleri incelenmiştir.

Bu çalışmada öncelikle farklı ülkelerin kurup sürdürdüğü çeşitli navigasyon sistemlerinden bahseldilmiş, bu sistemlerde kullanılan sinyaller, bant genişlikleri, modülasyon teknikleri gibi özellikler incelenmiştir.

Günümüzde yazılım tabanlı radyolar gibi RF sinyal yayını yapan modüller yaygınlaştığı için aldatma saldırıları da gün geçtikçe gelişmiştir. Bu yüzden aldatma karşıtı bir alıcı mimarisi için öncelikle tehditlerin analizi ve bu tehditlerin teknik detaylarının bilinmesi gerektiğinden dolayı; GNSS sistemlerinin özelliklerinin çalışılmasının ardından çeşitli aldatma yöntemleri ve teknikleri incelenmiştir. Bu teknikler sınıflandırılmış ve bu tekniklerin uygulamalardaki zorlukları ve etkileri değerlendirip çizelgeler şeklinde paylaşılmıştır. Ayrıca, aldatma karşıtı yöntemler değerlendirilmiş ve bu yöntemler ile beraber bir entegre mimari önerilmiştir.

GNSS alıcılarının aldatmaya karşı dayanıklılığını artıran çeşitli yöntemler ve aldatma saldırılarına karşı denk gelen teknikler bulunmaktadır. Bu yöntemler kriptografik, anten tabanlı, INS/IMU tabanlı veya çoklu sensör yöntemleri gibi farklı veri kaynaklarının entegrasyonu ile ele alınmaktadır. Mevcut teknolojiler ve gelecekteki eğilimlerin kapsamlı bir analiziyle bu çalışma; GNSS'e giderek daha bağımlı hale gelen bir dünyada, gelişen tehditlere karşı GNSS aldatma karşıtı stratejilerde yeniliğin sürdürülmesinin önemini vurgulamayı amaçlamaktadır.

2. GPS/GNSS SİSTEMLERİ VE ALDATMA

2.1. GPS/GNSS Sinyallerine Genel Bakış

GNSS Küresel Navigasyon Uydu Sisteminin (Global Navigation Satellite System) kısaltılmasıdır. Bu sistemler dünya genelinde veya yakın çevresinde herhangi bir yerde konum ve zaman bilgisi sağlayan uydu tabanlı bir navigasyon sistemidir. En çok bilinen GNSS sistemi GPS'dir (Global Positioning System- Küresel Konumlandırma Sistemi) ve bu sistem ABD tarafından işletilmektedir [3]. Bunun yanı sıra farklı ülkeler ve kuruluşlar tarafından geliştirilen ve sürdürülen birkaç farklı GNSS sistemi bulunmaktadır. Ülkelerin geliştirdiği sistemlerin listesi ve frekans bantları çizelge halinde aşağıda belirtilmiştir.

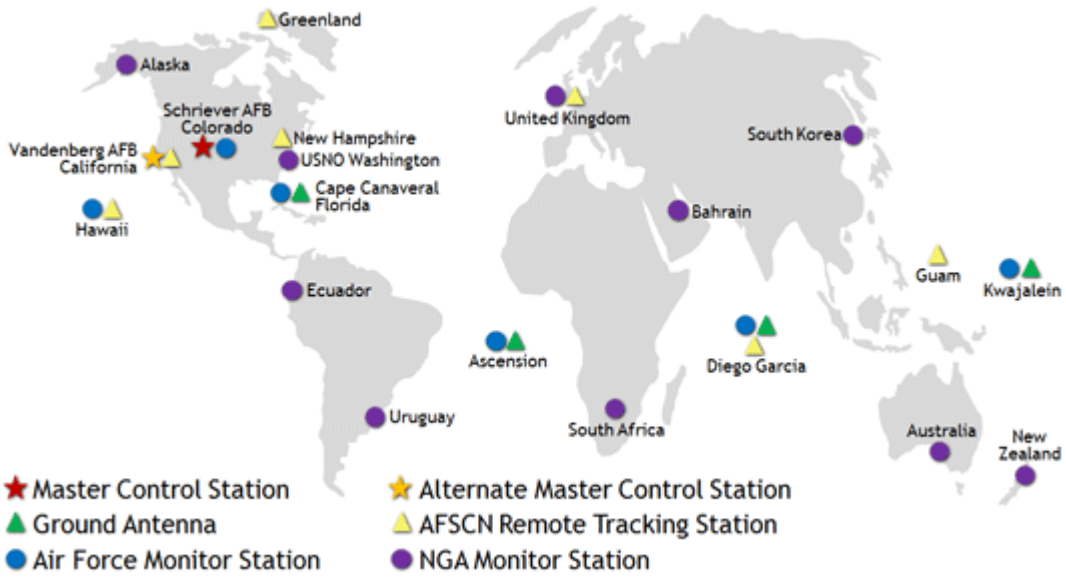
Çizelge 2.1 - GNSS sinyalleri ve frekans bantları

Sistem	Menşei	Frekans Bantları (GHz)
BeiDou	Çin	B1: 1.561098 B1-2: 1.589742 B2: 1.20714 B3: 1.26852
Galileo	Avrupa Birliği	E1: 1.559–1.592 E5a/b: 1.164–1.215 E6: 1.260–1.300
GLONASS	Rusya	G1: 1.593–1.610 G2: 1.237–1.254 G3: 1.189–1.214
GPS	ABD	L1: 1.563–1.587 L2: 1.215–1.2396 L5: 1.164–1.189

GNSS sistemlerinin genel olarak temel işleyişi, uzaydaki uydu segmenti, yere yerleştirilmiş kontrol segmenti ve kullanıcı segmenti arasında etkileşimleri içerir.

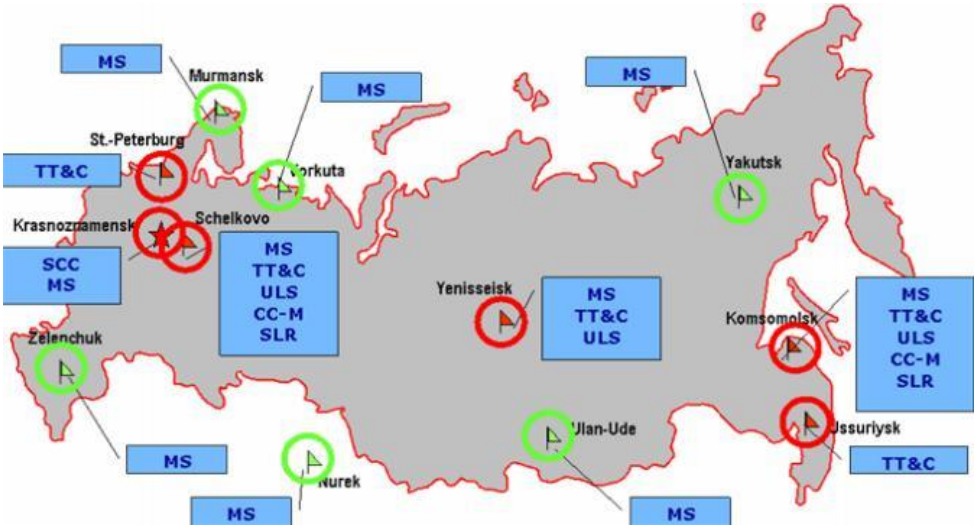
Uzay Segmentini açıklamak gerekirse GNSS sistemleri, Dünya yörüngesinde dönen bir dizi uydu tarafından oluşturulan bir uzay segmentine sahiptir. Bu uydu grubu, düzenli aralıklarla dünya etrafında döner ve sürekli olarak uyduların konum ve zaman bilgilerini yayınlar. Uzay segmenti, uydu sayısı ve dağılımıyla GNSS sistemlerin küresel kapsamını sağlar. Örnek vermek gerekirse şu anda operasyonel olarak 31 adet GPS uydusu bulunmaktadır ve bunların dünyadan yükseklikleri yaklaşık olarak 20200 km dir [4]. Aynı şekilde Rusya tarafından yürütülen GLONASS systeminin de 24 adet uydusu bulunmaktadır ve GPS uyduları ile yaklaşık olarak aynı yüksekliktedir [5].

Kontrol Segmenti, uydu sistemini yöneten ve izleyen kontrol merkezlerini içeren altyapılardır. Bu merkezler, uydu konumlarını doğrulamak ve zaman senkronizasyonunu sağlamak için sürekli olarak uydu sinyallerini izlerler. Ayrıca, uydu yörüngelerini düzeltmek ve uydu saatlerini doğru tutmak için düzeltmeler yaparlar. Kontrol segmenti, GNSS sistemlerinin doğru ve güvenilir çalışmasını sağlamak için gerekli düzenlemeleri gerçekleştirir. Bu segment, GNSS uydu ağının yönetimini ve izlenmesini sağlar. GPS için başlıca kontrol merkezleri arasında Colorado Springs, Colorado'daki Schriever Hava Kuvvetleri Üssü'ndeki GPS Operasyonel Destek Merkezi (GPS Operations Center) ve Colorado Springs'teki GPS Ana Kontrol İstasyonu (GPS Master Control Station) bulunur [6]. Bununla birlikte, dünya genelinde bir dizi izleme istasyonu da bulunmaktadır.



Şekil 2-1 GPS Kontrol Segmenti Konumları

GLONASS sisteminin kontrol segmenti bileşenlerinin neredeyse tamamı (Brasilia, Brezilya'daki bir istasyon dışında) eski Sovyetler Birliği toprakları içinde yer almaktadır [7].



Şekil 2-2 GLONASS Kontrol Segmenti Konumları

Kullanıcı Segmenti, GNSS alıcılarını içerir ve GNSS sinyallerini alarak konum ve zaman bilgilerini hesaplar. GNSS alıcıları, en az dört uydu sinyalini aynı anda alarak kendi konumunu belirler. Bu konumlandırma süreci, GNSS alıcısının uzaydaki uydu konumlarından kaynaklanan sinyallerin zamanlama farklılıklarını kullanarak gerçekleştirilir. GNSS alıcıları alınan sinyallerin şifrelemesini çözerek ve konum hesaplamalarını yaparak kullanıcılara güvenilir konum, hız ve zaman bilgilerini sağlar.

2.2. GPS/GNSS Sinyallerinin Teknik Özellikleri

Bu başlık altında GPS/GNSS sinyallerinin yapısı, frekans bantları gibi teknik özellikler detaylı bir şekilde incelenmiştir.

2.2.1. GPS Sinyalleri

GPS sinyal yapısı, GPS uydu sisteminden yayılan ve kullanıcı cihazlar tarafından alınan sinyalleri kapsar. GPS uydu sistemleri L1(1575.42 MHz), L2 (1227.60 MHz) ve L5 (1176.45 MHz) bantlarında sinyal yayınlar. L1 bandı, sivil kullanım için temel

taşıyıcı frekansını temsil ederken, L2 ve L5 bantları daha gelişmiş sinyal işleme ve doğrulama özelliklerini içerir [3].

Her GPS sinyalinin temel olarak 3 tane bileşeni vardır. Bunlar;

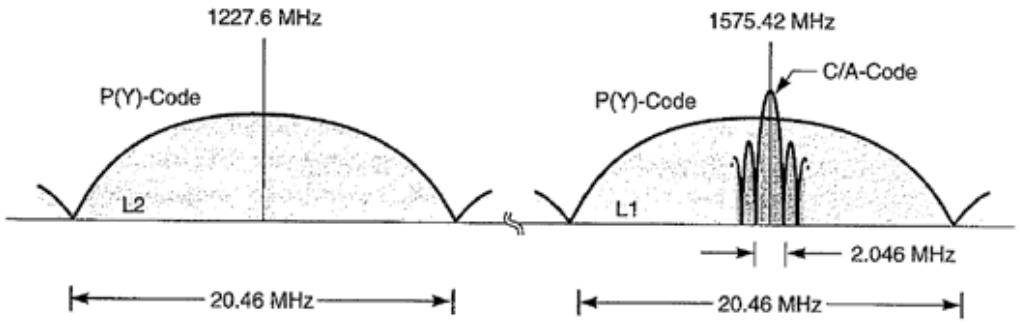
Carrier (Taşıyıcı)

Ranging Code (Menzil Kodu)

Navigation Data (Navigasyon Verileri)

Bu başlıklar aşağıda detaylı şekilde incelenmiştir.

Carrier (Taşıyıcı), L1, L2 veya L5 bantlarında bulunan RF sinüzoidal sinyali ifade eder. Uydularda bulunan atomik osilatör standardı 10.23 MHz olduğu için 1575.42 MHz olan L1 bandı standardın 154, 1227.60 olan L2 bandı standardın 120, 1176.45 MHz olan L5 bandı standardın 115 tam katıdır.



Şekil 2-3 GPS L1 ve L2 Bandında Bulunan Sinyallerin Spektrumları

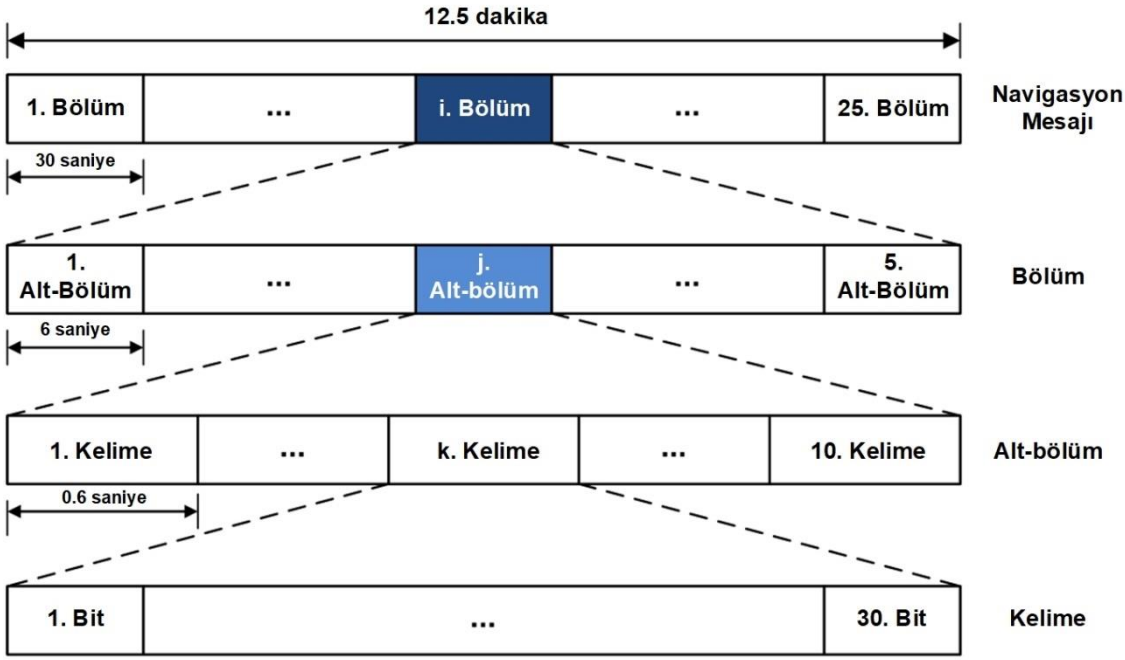
Ranging Code (Menzil Kodu), bir alıcı ve bir verici arasındaki mesafeyi ölçmek için kullanılan bir kodlama sistemidir. Ayrıca uydular PRN (Pseudo Random Noise) kodu da denilen kendine özel ve benzersiz bir kod gönderirler ve bu kodun öyle bir matematiksel özelliği bulunmaktadır ki uydular birbirleri ile girişime girmeden bu kodları aynı frekansta gönderebilmektedirler. Bu kodlar doğru konum hesaplamasına olanak sağlar ve GPS anteni tarafından alınan, yansıyan ve girişime uğramış sinyallerin bozucu etkilerini azaltır. SPS kodlarına sivil sinyaller olan C/A kodları, PPS kodlarına da kriptolu olan P(Y) kodları denilmektedir. Her bir uydu L1,

L2 ve L5 bandında benzersiz bir C/A kodu, L1 ve L2 bandında da benzersiz bir P(Y) kodu gönderir [3].

Her bir C/A kodu benzersiz 1023 bitlik bir dizidir ve 1 milisaniyede kendini tekrar eder. Yani 1 milisaniyede yaklaşık 1023 bit gönderildiği için her bir chip'in süresi yaklaşık 1 mikro saniyedir. Chip frekansı da 1 milisaniyede 1023 bit gönderildiği için saniyede 1023000 bit gönderebilir ve bu yüzden 1.023 MHz dir.

P-code ise 1014 chipten oluşan aşırı uzun PRN dizisinin benzersiz bir segmentidir. Chip frekansı 10.23 Mcps dir. Yani C/A kodundan 10 kat daha fazladır. Chip genişliği de yaklaşık 30 m dir. P-codu haftada 1 tekrar eder. P-code gizlidir. Hiçbir kamuya açık dokümanda bu kod net olarak tanımlanmamıştır.

Navigation Code (Navigasyon Kodu), uydunun sağlık durumu, pozisyonu, hızı, saat bias parametreleri ve almanac verileri gibi verileri kodlanmış şekilde sunan verilerdir. Navigasyon kodu saniyede 50 bit hızı ile aktarılır [8].



Şekil 2-4 GPS Navigasyon Mesajı İçeriği

Şekil 2-4’te görüldüğü gibi navigasyon mesajının içeriği toplamda 1500 bit uzunluğundadır. 1 navigasyon mesajında 30 saniyelik 25 adet bölüm vardır. Her bir bölüm 5 adet her biri 6’şar saniyelik alt-bölümlerden oluşur. Herbir alt-bölüm ise 0.6’şar saniyelik 10 adet kelimeden oluşur. 1 kelime de Şekil 2-4’te görüldüğü gibi 30 bitten oluşur. Buradan hareketle 1 alt-bölüm toplamda 300, 1 bölüm 1500, 1 navigasyon mesajı ise 37500 bitten oluşmaktadır.

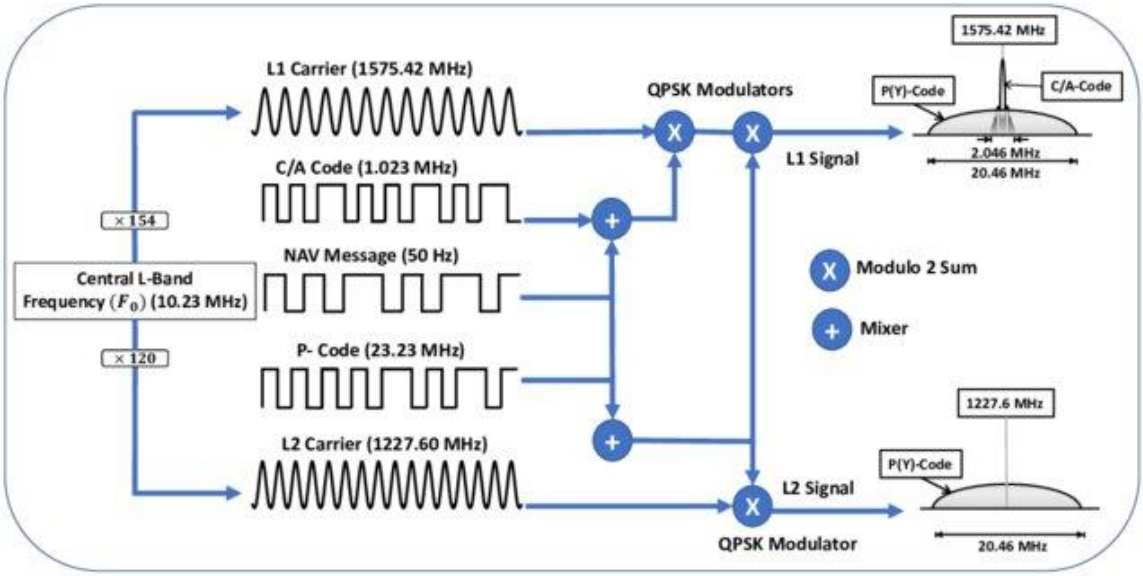
Herbir bir alt-bölümün birinci ve ikinci kelimeleri sırasıyla telemetri (TLM) ve HOW (Handover-Word) kelimeleridir.

Telemetri, GPS uydularından alınan veri akışını ifade eder. GPS telemetri verileri, uydunun durumu, yörüngesi, sağlık durumu, sıcaklık ve diğer mühendislik parametreleri gibi önemli bilgileri içerir. Bu veriler, hem uyduların kontrolü için hem de GPS alıcılarının doğru konum belirlemesi için kullanılır. Telemetri verileri, genellikle yer istasyonları tarafından alınır ve uydu performansını izlemek için analiz edilir.

"Handover Word" (HOW), GPS sisteminde kullanılan ve alıcıların veri senkronizasyonunu sağlamasına yardımcı olan bir terimdir. Bu terim, alıcının GPS veri akışını doğru bir şekilde anlamlandırmasına yardımcı olur. HOW, GPS mesajındaki zaman bilgilerini senkronize etmek için de kullanılır, böylece alıcı uydu sinyalini doğru bir zaman diliminde okuyabilir ve doğru konum hesaplamaları yapabilir.

Alt-bölümlerin birinci ve ikinci kelimelerinin dışındaki kelimeleri farklı verileri içerir. Birinci alt-bölüm uydu saat durumunu, saat düzeltmelerini ve uydu sağlık durumunu içerir. İkinci ve üçüncü alt-bölümler ise efemeris verilerini içerir. Dördüncü alt-bölüm iyonosferik model parametreleri, UTC bilgileri, almanac verisinin bir kısmı ve Anti-Spoofing (A/S) etkin olup olmadığını (P kodunu şifreli Y koduna dönüştüren) belirten göstergeleri sağlar. Beşinci alt-bölüm ise almanac ve konstelasyon durumunu içerir.

Şekil 2-5’ de görüldüğü gibi PRN code ile Nav Data XOR lanıyor. Yani Eğer 2 binary kodda aynıysa 0, farklıysa 1 sonucu elde ediliyor. Ardından çıkan sonuç ile RF taşıyıcı modüle ediliyor ve bu modülasyon da BPSK (Binary Phase Shift Keying) dir. 0 sinyalde bir şey değiştirmezken 1 sinyali -1 ile çarpıp fazını 180 derece kaydırıyor.



Şekil 2-5 GPS Sinyal Üretim Süreci

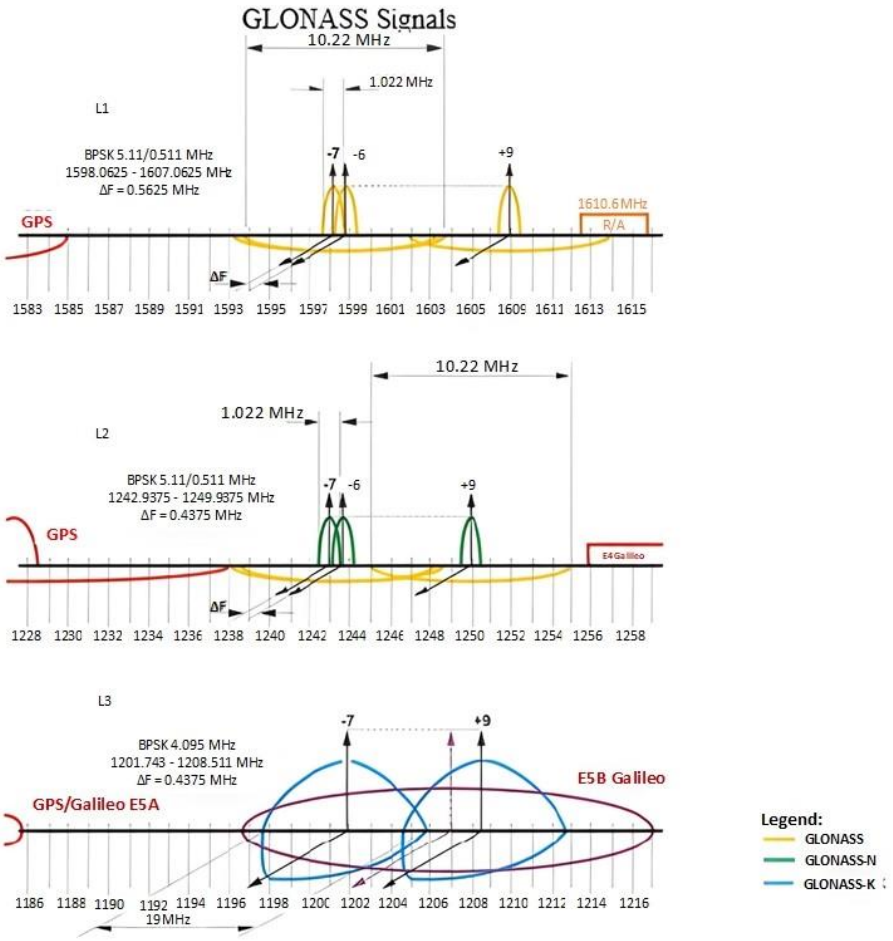
2.2.2. GLONASS Sinyalleri

GLONASS, Rusya tarafından geliştirilen ve işletilen küresel bir navigasyon sistemidir. GLONASS, GPS (Global Positioning System) sistemi gibi dünya genelindeki kullanıcılara konum bilgisi sağlamak üzere tasarlanmıştır. GPS'te olduğu gibi GLONASS da uzay segmenti, kullanıcı segmenti ve kontrol segmentinden oluşur. Uzay segmentinde 27'den fazla uydu bulunmaktadır ve her bir uydu kendi yörüngesinde dönerek dünya üzerinde farklı yerleri kapsar.

GLONASS'ta GPS'ten farklı olarak her uydu farklı frekansta aynı kodu gönderir. GPS'te her uydu aynı frekansta farklı kod gönderir ve bu Code Division Multiple Access(CDMA) ile yapılır. Fakat GLONASS'ta her uydu aynı kodu gönderir ve kendine ait bir frekansta Frequency-Division Multiple Access (FDMA) yöntemi ile yapmaktadır. Şekil 2-6 görselde GLONASS sinyallerinin spektrumları gösterilmiştir.

Üç farklı GLONASS L frekansı bandı, uydulara atanacak farklı bir frekans aralığına sahiptir. GLONASS taşıyıcı frekansları üç alanda kullanır. Birincisi, bireysel taşıyıcı frekanslar arasındaki ayrımın 0,5625 MHz olduğu L1 bandıdır ve frekansı yaklaşık olarak 1602 MHz ve frekans aralığı 1598.0625 ila 1607.0625 MHz dir. İkincisi, bireysel taşıyıcı frekanslar arasındaki ayrımın 0,4375 MHz olduğu L2 bandıdır ve frekansı yaklaşık 1246 MHz ve frekans aralığı 1242,9375 ila 1249,9375 MHz dir. Üçüncü frekans bandı ise L3'tür. L3'teki bu üçüncü sivil sinyal, GLONASS'ın

modernizasyonu kapsamında gönderilen K uydularında ve 1201.743 ila 1208.511 MHz'yi içeren yeni bir frekans bandında mevcuttur ve Galileo'nun E5B sinyaliyle üst üste gelmektedir. L3'te bireysel taşıyıcılar arasında 0,4375 MHz'lik bir ayrım vardır. Bununla birlikte, bu aralıklar içerisinde L-bant sinyallerinin 25'e kadar kanalı olabilir; şu anda mevcut uydulara uyum sağlamak için her birinde 16 kanal bulunmaktadır.



Şekil 2-6 GLONASS Sinyalleri Spektrumları

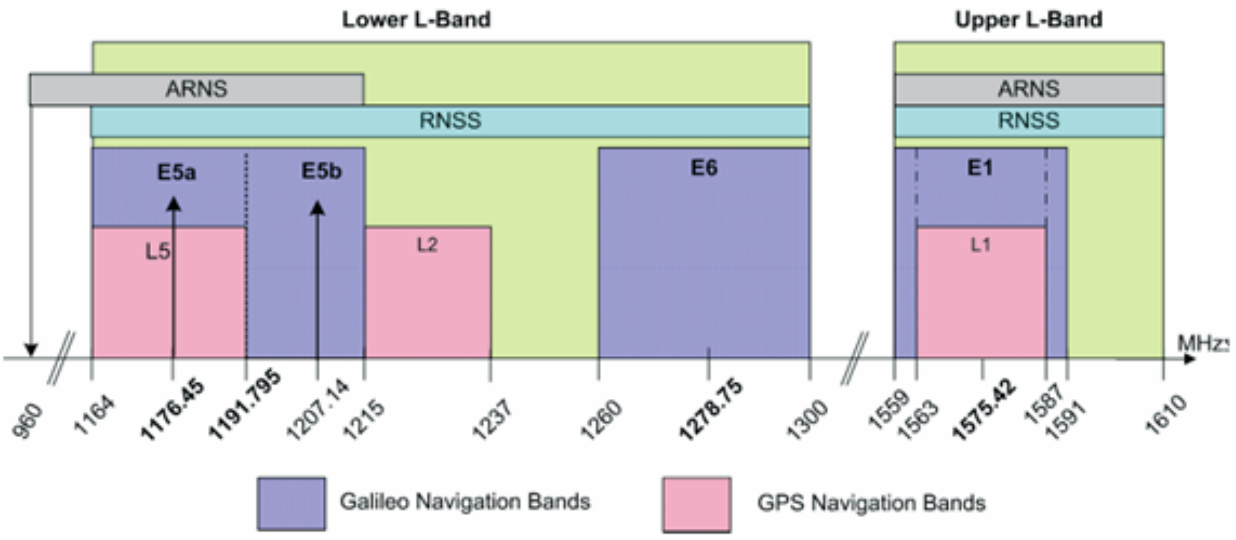
GLONASS L1 bandındaki chip frekansı standart konumlandırma için 0.511 MHz, hassas konumlandırma için 5.11 MHz'dir. L2 bandında da L1 bandında olduğu gibi chip frekansları standart ve hassas konumlandırma için sırasıyla 0.511 ve 5.11 MHz'dir. GPS'te olduğu gibi, GLONASS'ta da hassas ve standart konumlandırma

hizmetleri vardır ve hassas hizmet daha yüksek doğruluk gerektiren daha zorlu uygulamalar için ayrılmıştır.

2.2.3. Galileo Sinyalleri

Galileo Sistemi, Avrupa kontrolünde bir uydu tabanlı navigasyon sistemidir ve Galileo uyumlu alıcılarla donatılmış kullanıcılara çeşitli hizmetler sunmak için tasarlanmış bir sistemdir.

Toplamda dört çeşit Galileo sinyalleri bulunmaktadır. E5a, E5b, E6 and E1. E5a ve E1 mevcutta bulunan L1 ve L5 GPS sinyalleri ile üst üste gelir. Galileo sinyallerinden alınan en düşük güç -152 dBW'tır ve Şekil 2-7'de görüldüğü gibi bu da GPS'teki C/A kodlarının gücünden 2 katından daha fazladır.



Şekil 2-7 Galileo ve GPS Sinyalleri Gösterimi

Galileo'da toplamda 6 seviye navigasyon hizmeti bulunmaktadır. Bunlar açık hizmet (open service), ticari hizmet (commercial service), kamu düzenleme hizmeti (the public regulated service), arama ve kurtarma hizmeti (the search and rescue service), hayati güvenlik hizmeti (The Safety of Life Service), ve yüksek doğruluk hizmeti (high accuracy service) dir.

Çizelge 2.2 - Galileo servislerinin tanımı ve frekans bantları

Hizmet Adı	Tanımı	Kullandığı frekans bandı (MHz)
Açık Hizmet	Galileo uyumlu alıcılara sahip tüm kullanıcılar için ücretsiz bir hizmettir.	E1: 1575.42 E5a: 1176.45 E5b: 1207.14
Ticari Hizmet	Açık Hizmet'in üzerinde ek değerli hizmetler sunar, bunlar arasında daha yüksek veri hızları ve daha hassas konumlama bulunur.	E6: 1278.75 E1: 1575.42
Kamu Düzenleme Hizmeti	Hükümet tarafından yetkilendirilmiş kullanıcılar tarafından kullanılmak üzere tasarlanmış şifreli bir hizmettir	E1: 1575.42 E6: 1278.75
Arama Ve Kurtarma Hizmeti	Acil durum işaretlerinden gelen tehlike sinyallerinin tespit edilmesini ve yerinin belirlenmesini sağlar.	Yer- uydu bağı: 406 Uydu- yer bağı: 1544.1
Hayati Güvenlik Hizmeti	Havacılık ve denizcilik navigasyonu gibi güvenliğin kritik olduğu uygulamalara yöneliktir.	E1: 1575.42 E5a: 1176.45
Yüksek Doğruluk Hizmeti	Açık hizmet sinyallerine düzeltmeler sağlayarak gerçek zamanlı, yüksek hassasiyetli konumlama sunar.	E6: 1278.75

2.2.4. BDS (Beidou)

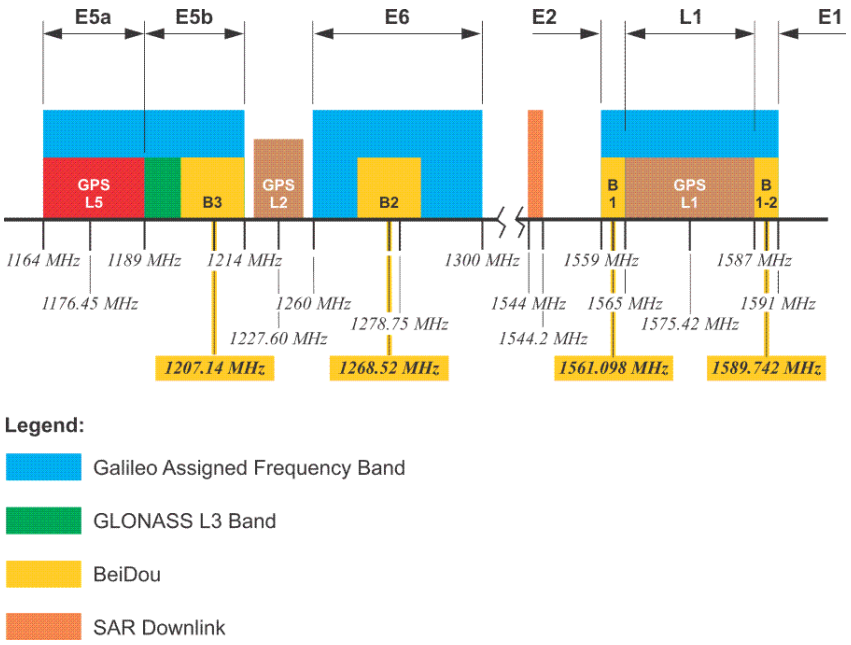
Beidou Navigasyon Uydu Sistemi (BDS), Çin Ulusal Uzay İdaresi tarafından geliştirilen ve işletilen bir uydu tabanlı radyo navigasyon sistemidir [9]. Sistem, yeryüzündeki veya yakınındaki BDS alıcısına dört veya daha fazla BDS uydusunun engelsiz görüş hattı olduğu yerlerde coğrafi konum ve zaman bilgisi sağlayabilir. Kullanıcının herhangi bir veri iletimi yapmasına gerek yoktur ve sistem, telefon veya internet alımına bağımlı olmadan çalışabilir, ancak bu teknolojiler BDS konumlandırma bilgisinin kullanışlılığını artırabilir.

Beidou-1 (ilk nesil Beidou) sistemi, üç uydudan oluşur ve başlangıçta Çin içinde bölgesel konumlandırma hizmetleri sunmuştur [9]. Beidou-2 (ikinci nesil Beidou) sistemi, 16 uydu içerir ve bunlar arasında 6 jeostasyoner uydu, 6 eğik jeosenkron yörüngeli uydu ve 4 orta Dünya yörüngeli uydu bulunur. Beidou-2, Kasım 2012'den itibaren Asya-Pasifik bölgesinde kullanıcılara bölgesel konumlandırma hizmetleri sağlamaya başlamıştır. Bölgede GPS'ten daha hassas olduğu belirtilmiştir.

Beidou-3 (üçüncü nesil Beidou) sistemi, farklı yörüngelerdeki uydulardan oluşur ve 2020 Temmuz'unda tamamen işlevsel hale gelmiştir. Bu sistem, GLONASS, Galileo ve GPS gibi diğer küresel konumlandırma sistemleriyle birlikte, dünya çapında zamanlama ve navigasyon için tam kapsama alanı sağlar.

Çin, BDS üzerinden, Çin ve çevresindeki bölgelere ücretsiz hassas nokta konumlama hizmetleri, kısa mesaj iletişim hizmetleri ve arama ve kurtarma hizmetleri sunmaktadır. BDS ayrıca, yüksek hassasiyetli konumlandırma hizmetleri sunan Yer Takviye Sistemi (GAS) hizmeti de sunmaktadır. BDS, 2020 yılı itibarıyla birçok alanda yaygın olarak kullanılmakta ve 120'den fazla ülke ve bölgede BDS ürünleri kullanılmaktadır.

Beidou uyduları, üç frekans bandında sinyaller yayınlar; B1 (1561.098 MHz), B2 (1207.14 MHz) ve B3 (1268.52 MHz). Bu sinyaller, Galileo'nun E1, E5B ve E6 frekans bantları ile örtüşür. Her Beidou sinyali, bu bantlarda bir I (in-phase) ve Q (quadraphase) bileşeni içerir ve CDMA çoklu erişim sistemini kullanır. Modülasyon şeması olarak dört fazlı kaydırma anahtarı (QPSK) kullanılır. Beidou Radyo Navigasyon Uydu Servisi (RNSS), beş yeni küresel sinyal içerir; B1C (1575.42 MHz), B1A (1575.42 MHz), B2a (1176.45 MHz), B2b (1207.14 MHz) ve B3A (1268.52). Bu frekans bantları, GPS L1 ve Galileo E2-L1-E1, GPS L5 ve Galileo E5a, Galileo E5b ve Galileo E6 ile örtüşür.



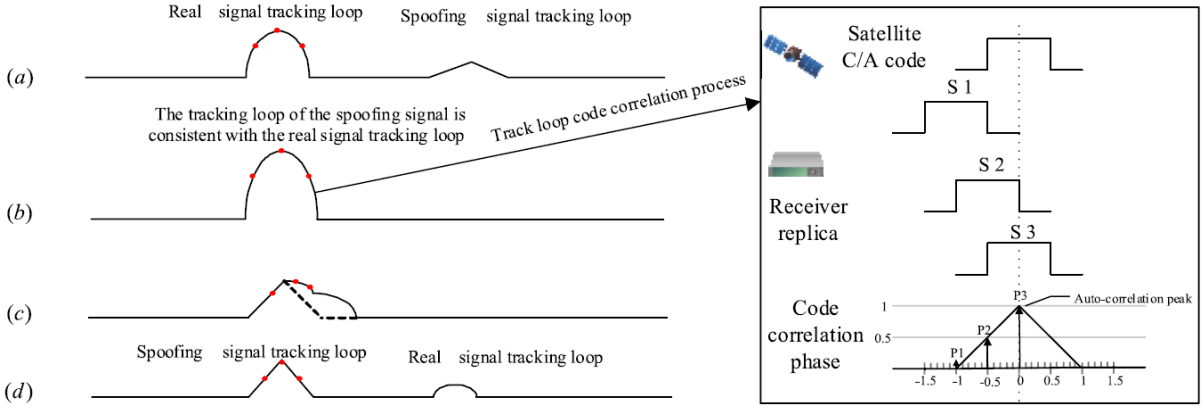
Şekil 2-8 BeiDou, Galileo ve GLONASS Sinyalleri Frekans Bandları

2.3. GPS/GNSS Aldatma

Birçok GNSS alıcısı için uydudan alınan sinyal gücü çok zayıftır ve kasıtlı veya kazara oluşan parazitlerden kolayca etkilenebilir. Sivil GNSS'ye ait Arayüz Kontrol Belgesi (ICD), sivil uydu navigasyon sinyalleri için taşıyıcı frekansı, modülasyon modu, navigasyon mesajı gibi ilgili parametrelerin ayrıntılı açıklamalarını içerir [10], [11]. Uydu sinyallerinin alınması ve izlenmesi genellikle yayılma kodu korelasyonu (spreading code correlation) ile belirlenir. Ancak pratikte, çoklu yol etkileri ve bozucu sinyaller, alıcının uydu sinyallerini normal bir şekilde almasını etkileyebilir. Çoklu yol etkisi ile gelen sinyalinin gücü, gerçek sinyalin gücünden daha az olduğundan, GNSS alıcısı daha düşük güçlü sinyalin gürültü olduğunu kabul eder ve çoklu yol etkisine karşı koymak için daha yüksek güçlü sinyali izler. GNSS aldatıcı, alıcı mekanizmasını kullanarak aldatma sinyalinin gücünü, gerçek sinyal gücünden biraz daha büyük olacak şekilde ayarlar ve GNSS alıcısı çoklu yol etkisine karşı koymak için gerçek sinyali gürültü gibi, taklit sinyali ise gerçek sinyal gibi algılar. Böylece aldatıcı, GNSS alıcısını aldatma amacına ulaşır. Genel olarak Şekil 2-9'da görüldüğü gibi aldatma sinyalinin dört tür aldatma süreci diyagramı tanıtılmaktadır.

GNSS aldatmada, gerçek sinyal ve aldatma sinyalinin dört modu vardır. Bu modlar Şekil 2-9'da gösterilmiştir. Eğri (a) aldatma sinyalinin, gerçek sinyalin izleme

döngüsünü aradığı süreci temsil eder ve aldatma sinyalinin gücü, gerçek sinyalin gücünden azdır. Eğri (b) aldatma sinyalinin izleme döngüsünün gerçek sinyalin izleme döngüsüyle tutarlı olduğunu gösterir. Eğri (c) alıcının gerçek sinyal durumunu yakalamaktan aldatma sinyal durumunu yakalamaya geçişini gösterir. Eğri (d) aldatma sinyal gücünün gerçek sinyal gücünden büyük olduğunu ve iki tür sinyal arasında belirli bir faz farkı olduğunu belirtir.



Şekil 2-9 GNSS Alıcılarını Aldatma Aşamaları

Bu şekilde, alıcı düşük güçlü gerçek sinyalin gürültü altında bir yan ürün olduğunu yanlış bir şekilde kabul eder. Bu durumda, alıcı sürekli olarak aldatma sinyaline kilitli kalır. Faz farkı nedeniyle, alıcı alınan sinyalin bir aldatma sinyali olduğunu anlamakta zorlanır. Aldatma süreci genellikle eğri (a) ile eğri (d) arasında gösterilir. Şekil 2-9' nin sağ kısmı, uydu C/A kodunun alıcının kopya koduyla nasıl ilişkili olduğunu gösterir. S1'den S3'e kadar, alıcının kopya kodunun üç faz durumudur. Aldatma saldırılarının başarısını daha da artırmak için, aldatma yapan taraf belirli aldatma stratejilerini de birleştirmelidir. Mevcut aldatma sistemleri ve bu sistemler için kullanılan stratejiler ilerleyen sayfalarda sınıflandırılıp detaylandırılacaktır.

Esas olarak uydu tabanlı konum alıcılarına yapılan saldırı sistemlerini iki ana başlığa bölebiliriz. Bunlar karıştırma (jamming) saldırısı ve aldatma (spoofing) saldırısıdır. Karıştırma saldırısı sinyalin alınmasını önleyen [12] ve alıcı tarafından kolayca tespit edilebilen bir yöntemdir. Bu yüzden aldatma saldırıları daha çok önem arz etmektedir. Aldatma saldırısını da iki kategoriye ayırabiliriz; kopyalamalı aldatma (forwarding spoofing) saldırısı ve üretici aldatma (generating spoofing) saldırısı.

Aldatma saldırılarına, kopyalamalı aldatma saldırısını inceleyerek başlayabiliriz. Bu saldırı türü, uydudan gelen sinyali kopyalayarak GNSS alıcısına yanlış sinyalin gelmesini sağlamaktır [13]. Bu şekilde eğer çeşitli aldatma stratejileri kullanılarak yapılırsa uydu sinyali ile senkron olacağından dolayı tespitinin de kolay olmayacağı ve ayrıca askeri sinyallerde de bu aldatmanın yapılabileceği çeşitli makalelerde anlatılmıştır [14]. Diğer bir saldırı türü olan üretici aldatma saldırısında ise doğrudan uydu sinyali üretilip taklit edilir ve bu üretilen sinyalin yayını yapılır. Yapılan bu yayın GNSS alıcısına ulaştırılır.

Sinyalleri askeri sinyaller ve sivil sinyaller olarak iki kategoriye ayırmak mümkündür. Askeri ve sivil sinyallerde karıştırma saldırısının uygulanması zor değildir ve mevcut uydu sinyallerine girişimi çok güçlüdür. Fakat karıştırma saldırısı GNSS alıcılar tarafından kolayca tespit edilebilir. Tespit edildikten sonra uygun tedbirler ile karıştırma saldırısına karşı konulabilir.

Askeri ve sivil sinyaller üzerinde kopyalamalı aldatma saldırısını uygulamanın zorluk derecesi düşüktür. Fakat kopyalamalı aldatma saldırısını tek başına yapmak etkili olmayabilir. Ayrıca kopyalamalı aldatma saldırısı tek başına uygulanırsa alıcı taraf navigasyon mesajının özelliklerinden bir aldatma saldırısı gerçekleştiğini algılayabilir. Bu yüzden kopyalamalı aldatma saldırısını birkaç aldatma stratejisi ile birleştirip uygulamak, aldatma saldırısının başarısını yüksetme açısından oldukça önemlidir. Bunlara ek olarak, kopyalamalı aldatma saldırısında konum keyfi olarak kontrol edilemez.

Askeri GNSS sinyalleri hiçbir kamuya açık dokümanda net olarak tanımlanmaz. Bu yüzden üretici aldatma saldırısı, askeri sinyallere uygulanabilen bir saldırı türü değildir. Fakat sivil GNSS sinyalleri, ilgili navigasyon arayüz kontrol dokümanları veya ilgili sistem dokümanlarından bulunabileceğinden dolayı bu saldırı türü ile GNSS alıcılarına istenilen zaman/konum bilgisi gönderilebilir.

Aldatma stratejileri ise 4 başlık altında toplanabilir.

- Tekrarlayarak Aldatma Saldırısı (Replay Spoofing Attack (RSA))
- Taklit Ederek Aldatma Saldırısı (Forgery Spoofing Attack (FSA))
- Kestirimci Aldatma Saldırısı (Estimation Spoofing Attack (ESA))
- İleri Seviye Aldatma Saldırısı (Advanced Spoofing Attack (ASA))

Tekrarlayarak aldatma saldırısında aldatma yapan taraf, alınan sinyalin üzerine gecikme ekleyerek alıcıyı aldatmaya çalışır. Bu tür bir aldatmanın uygulanması nispeten basittir. Ancak, aldatıcı bu yöntemle aldatma başarısını artırmak istiyorsa, aldatma sinyal parametrelerini makul bir şekilde ayarlamalı ve uygun aldatma ortamını sağlamalıdır. Böylece daha iyi bir aldatma etkisi elde edilebilir. Bu aldatma saldırısının uygulamadaki zorluğu nispeten basittir ve saldırı etkisi orta derecelidir.

Taklit ederek aldatma saldırısında aldatıcı, bir aldatma sinyali üreterek sinyalin ilgili parametrelerini ayarlar ve böylece aldatıcı, alıcının bulduğu konum sonucunu kotrolü altına alır. Bu aldatma saldırısının uygulamadaki zorluğu tekrarlayarak aldatma saldırısına göre orta derecededir ve saldırı etkisi de daha yüksek, orta-iyi arasındadır.

Kestirimci aldatma saldırısı sadece sıradan sivil sinyalleri etkilemekle kalmaz, aynı zamanda bilinmeyen güvenlik kodlarına sahip bazı sivil uydu sinyallerini de aldatabilir. Bu yöntem, sinyal kestirimi yoluyla uydu bilgilerini kestirir ve sinyal kestirimi sonucu ile uydu sinyalleri üreterek sinyal alıcısını kontrol eder. Diğer aldatma saldırılarına göre kestirimci aldatma saldırısının uygulanması zordur fakat saldırı etkisi diğer aldatma saldırılarına göre iyidir.

İleri seviye aldatma saldırısında daha karmaşık ve aldatma karşıtı yöntemler kullanan alıcılar için, aldatıcı sadece birden fazla aldatma stratejisi benimsemekle kalmaz, aynı zamanda daha doğrudan ve etkili bir aldatma sinyal formatı tasarlamak için sinyal özelliklerini de birleştirir. Bu şekilde alıcı daha etkili bir şekilde aldatılır. İleri seviye aldatma saldırısınının uygulanması karmaşık yöntemler içerdiğinden diğer aldatma saldırılarına göre oldukça zordur. Saldırı etkisi de bir o kadar fazladır.

2.3.1. Tekrarlayarak Aldatma

Uydudan gelen sinyaller kullanılarak yapılan saldırılar genel bir başlık olarak tekrarlayarak aldatma saldırısı şeklinde adlandırılabilir [15][16]. Uydudan gelen sinyale verilen etkiye göre 4 başlık altında incelenebilir. Eğer uydudan gelen sinyalleri doğrudan yayıyorsa buna doğrudan tekrarlayarak aldatma (direct replay spoofing attack**)** denilmektedir. Bu aldatma yöntemi ile sinyallere biraz gecikme katıldığı için bir aldatma yaratsa da zayıf aldatma etkisinden dolayı çok kullanılmamaktadır. Eğer uydudan gelen sinyal genliği artırılıp alıcıya bu sinyal

gönderilirse buna yüksek güçle tekrarlayarak aldatma (high power replay interferance) denilmektedir. Genliği artırılmış sinyali alan alıcı bu sinyali gerçek, gerçek sinyali de gürültü olarak görür. Bu metot genelde tek başına kullanılmaz ve aldatma saldırısının başarı oranını artırmak için başka yöntemler ile birleştirilerek kullanılır. Eğer uydudan gelen sinyale belli bir gecikme verilip basılırsa da bu saldırıya seçici gecikme ile tekrarlayarak aldatma (selective delay replay) denilmektedir. Bu metotta genelde aldatma saldırısının başarı oranını artırmak için başka metotlar ile birleştirilerek kullanılır. Son olarak çoklu anten ile aldatma (multi-antenna receiver replay interferance) saldırısı aldatıcı tarafından birkaç anten kullanarak tekrarlayarak aldatma saldırısının gerçekleştirilmesidir.

Esas olarak tekrarlayarak aldatma, uzun süreli yapıldığında sadece GPS sistemini değil INS-GPS sistemini de bozabilir. Genelde tekrarlayarak aldatma saldırıları raporun ilerleyen sayfalarında bulunan saldırılar ile beraber, saldırının başarı oranını artırmak için kullanılır.

Doğrudan tekrarlayarak aldatmada aldatıcı, alınan sinyali doğrudan ileten ve bu şekilde alıcının konumlama sonucunu etkilemeye çalışan bir sinyal tekrarlayıcısına benzer. Bu saldırının uygulanması oldukça basittir fakat kötü aldatma etkisi nedeniyle genellikle kullanılmaz.

Yüksek güçle tekrarlayarak aldatmada aldatıcı, aldatma sinyalinin gücünü yapay olarak artırarak alıcıyı aldatma sinyalinin gerçek bir sinyal olduğuna inandırır ve zayıf uydu sinyalinin çok yollu etki sonucu olduğunu düşünmesini sağlar. Böylece alıcıyı, aldatma sinyalini gerçek sinyalmiş gibi algılamasına yol açarak kandırır. Bu yöntemin uygulama zorluğu ve saldırı etkisi orta seviyededir. Bu yöntem genellikle aldatma başarısını artırmak için diğer stratejilerle birlikte kullanılır.

Gecikme ile tekrarlayarak aldatmada aldatıcı, aldığı uydu sinyaline yapay olarak belirli bir gecikme ekleyerek yayılma kodunun fazını ve alıcının yakaladığı uydu sinyalini etkiler. Bu yöntem de yüksek güçle tekrarlayarak aldatma yöntemi gibi uygulama zorluğu ve saldırı etkisi orta seviyededir ve bu yöntem genellikle aldatma başarısını artırmak için diğer stratejilerle birlikte kullanılır.

Çok antenli bir alıcı için, varış açısı anten tarafından tespit edilebilir. Eğer aldatma sinyali de tek antenli bir verici ile sinyal yayılımı sağlıyorsa, çok antenli alıcı bu aldatma sinyalini kolayca tespit edebilir. Bu nedenle, çok antenli bir alıcı için birden

fazla aldatma kaynağı gerekir ve aldatma etkisini artırmak için diğer aldatma stratejilerini birleştirmek gerekir. Bu yöntemin uygulamadaki zorluğu yüksektir fakat saldırı etkisi orta-iyi seviyesindedir.

2.3.2. Taklit Ederek Aldatma

Taklit ederek aldatma (forgery spoofing) saldırısı, yukarıda anlatılan tekrarlayarak aldatma saldırılarından daha karmaşıktır. Aslında taklit ederek aldatma yapabilen bir ekipmanda 3 tane modül bulunur. Bunlar; uydu sinyali alıcısı, aldatma sinyali oluşturma modülü ve aldatma sinyali gönderme modülüdür. Uydu alıcı modülü sinyali alır ve sinyal üretme kısmında 2 adet yöntem kullanabilir. Ya alınan uydu sinyalleri doğrudan basılır ve buna doğrudan üreterek aldatma (direct-generation forgery) denir [17]; ya da aldatıcı bu sinyalleri alıp demodüle edip gelen sinyalden ilgili parametreleri çıkartarak bu parametrelerle gerçek sinyale benzeyen bir sinyal üretir ki buna da analizle üreterek aldatma (analysis-generation forgery) denir [18] [19]. Eğer analizle üreterek aldatma saldırısında başarı oranını artırmak için sinyal seviyesi artırılarak gönderilirse buna da erişim engelleme ortamında aldatma (denial environment forgery) denilmektedir [20]. Eğer aldatıcı eşzamanlı olarak birden çok uydu sinyalini aldatıyorsa buna da tüm kanal aldatma (full-channel forgery) denilmektedir [21]. Tüm kanal aldatma saldırısı biraz karmaşık bir saldırı olduğu için bazı basit aldatma karşıtı önlemler bu saldırı karşısında başarısız olmaktadır.

Doğrudan üreterek aldatmada aldatıcı, çeşitli uydu navigasyon arayüz dosyaları aracılığıyla Alan Programlanabilir Kapı Dizisi (FPGA), Dijital Sinyal İşlemcisi (DSP) ve Yazılım Tanımlı Radyo (SDR) kullanarak doğrudan uydu sinyalleri üretir [22]. Ancak, doğrudan üretilen uydu sinyali, mevcut yayılmakta olan uydu sinyalinin faz farkı ve ilgili parametreleriyle eşleşmez ve bu nedenle alıcı tarafından kolayca alınmaz. Bu aldatma yönteminin uygulamadaki zorluk derecesi ve saldırı etkisi orta seviyededir.

Analizle üreterek aldatmada aldatıcı; sinyal vericisi, bir alıcı ve bir verici içerir. Alıcı, alınan gerçek uydu sinyalini analiz eder ve ardından elde edilen sinyal parametrelerini hemen iletilen aldatma sinyaline uygular, böylece aldatma başarısını artırır. Analizle üreterek aldatma saldırısının uygulamadaki zorluk

derecesi doğrudan üreterek aldatma saldırısına göre daha yüksektir. Saldırı etkiside doğrudan üreterek aldatma saldırısına göre daha iyidir.

Erişim engelleme ortamında aldatmada sinyal aldatma başarısını artırmak için aldatıcı, hedef alıcıya büyük ölçekli parazit gönderir. Bu da alıcıyı sıkıştırarak mevcut izleme doğruluğunu kaybetmesine neden olur. Bu durumda aldatıcı, aldatma sinyalini alıcı tarafından daha kolay alınacak şekilde gönderir, böylece aldatma amacına ulaşır. Bu aldatma yönteminin uygulamadaki zorluk derecesi ve saldırı etkisi orta seviyededir [23].

Tam kanal aldatma, bilinen tüm kanalların (veya hedef alıcının alabileceği kanalların) tam ölçekli aldatılmasıdır. Bu, aldatıcının aynı anda birden fazla uydu sinyalini kandırması gerektiği anlamına gelir. Bu durumda, aldatıcı alıcı konumlama sonucunu daha doğru bir şekilde kontrol edebilir. Tam kanal uydu sinyali aldatma saldırılarının karmaşıklığı nedeniyle, basit aldatma karşıtı stratejiler başarısız olacaktır. Bu aldatma yönteminin uygulamadaki zorluğu yüksektir fakat saldırı etkisi oldukça iyidir.

2.3.3. Kestirimci Aldatma

Aldatmaya karşı dayanıklı olan bazı navigasyon mesajları denilirken kastedilen, bu navigasyon mesajlarına navigasyon mesajının güvenliğini artırmak için bilinmeyen bir güvenlik kodu yerleştirilmesidir [24] [25]. Sadece üreterek aldatma saldırılarına dayalı aldatıcılar için bu saldırı bir işe yaramaz, çünkü aldatıcı güvenlik kodunu kestiremez ve bu yüzden alıcı tarafından tanınabilecek sinyali okuyup üretemez. Bu nedenle, aldatıcı alınan navigasyon mesajını kestirip kestirilmiş sinyaller ile alıcıyı yanıltmaya çalışır. Bu başlık altında son gelişmeleri de göz önünde bulundurursak iki tip saldırı vardır. Güvenlik Kodu tahmini ve tekrarlama (security code estimation and replay(SCER)) ve ileri kestirim saldırısı (forward estimation attack(FEA)). Eğer aldatıcı SCER saldırısını yapacaksa navigasyon mesajlarını, navigasyon sinyallerini ve sinyal kestirim yöntemlerini de bilmesi gerekmektedir. Bu saldırıda en önemli unsur, güvenlik kodunun kestirimini doğru yapmak ve yapay olarak eklenen beklemenin doğru kontrolüdür. Bu metot çok zor olduğu için gerçek projelerde genellikle kullanılmamaktadır.

FEA saldırısı, son yıllarda önerilen bir önceden tahmin yöntemidir. Çoğu alıcı, navigasyon mesajını çözmeden önce bu mesajı kontrol etmediği için aldatıcı, alıcıyı aldatmak için önceden bir bilgi edinip bu bilgi ile birleştirilmiş bir navigasyon mesajı oluşturabilir. FEA saldırısındaki navigasyon mesajı genellikle bir kimlik doğrulama işlevine sahip bir navigasyon mesajıdır. Doğal olarak, navigasyon mesajının içsel ilgisi nedeniyle aldatıcı tarafından elde edilen navigasyon mesajı bilgisi ne kadar fazlaysa, aldatıcı tarafından tahmin edilen yanıltıcı navigasyon mesajı o kadar doğru olacaktır. FEA'da, aldatıcı, sahte bilgiyi göndererek doğrulanmış bilginin gönderilmesinden önce bile aldatma sürecini uygulayabilir.

Buna karşılık, SCER önce doğrulanmış sinyali almalı ve ardından aldatma sürecini uygulayabilmek için sinyal parametrelerini tahmin etmelidir. [26] referans numaralı makalede FEA aldatma saldırısına yönelik simüle bir saldırı gerçekleştirildi, saldırı nesnesi bir Galileo sinyaliydi ve navigasyon mesajı doğrulaması (NMA) içeriyordu. Deneysel sonuçlar, FEA saldırısı altında NMA'nın kimlik doğrulama işlevini gerçekleştiremediğini göstermektedir. Bununla birlikte, gönderenin navigasyon mesajına anti-replay bilgisi eklemesi durumunda, her bir navigasyon mesajının bir kısmının farklı olması nedeniyle gelecekteki navigasyon mesajlarını tahmin etmeyi zorlaştırır. Yukarıdaki süreç, FEA saldırısına karşı belirli bir direnç sağlayabilir.

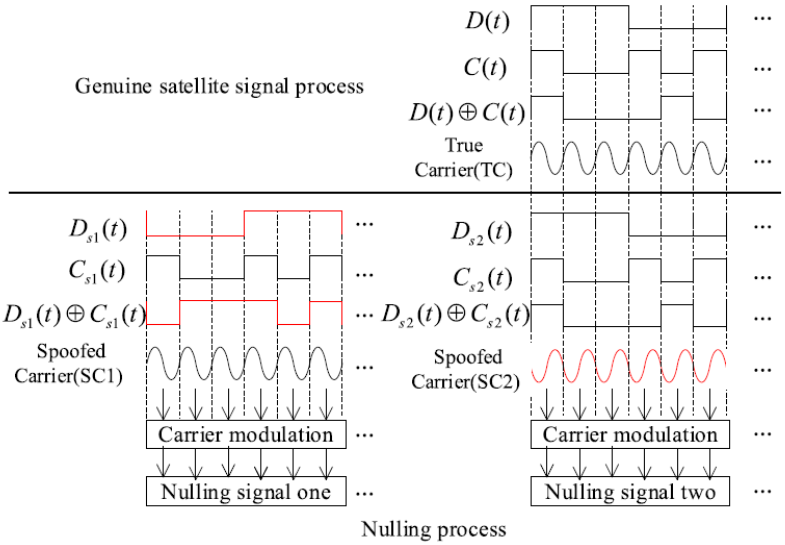
2.3.4. İleri Seviye Aldatma

Yukarıda bahsedilen aldatma teknikleri dışında son yıllarda bazı uzmanlar, içlerinde sıfırlama saldırısı (nulling attack) [27] ve işbirlikçi girişim (cooperative interferance attack) [28] saldırılarının da bulunduğu bazı aldatma saldırıları önermişlerdir.

Sıfırlama saldırısından bahsetmek gerekirse bu saldırı türü iki kısımdan oluşur.

Birinci sıfırlama sinyali uydudan gelen orijinal sinyali karıştıran ve hedef alıcının pozisyon ve zaman bilgilerini değiştirerek aldatma amacını başaran aldatma sinyalidir. Şekil 2-10 de görüldüğü gibi birinci sıfırlama sinyalinde uydu bilgisi farklı; menzil kodu ve taşıyıcı sinyalleri aynı kalmıştır. İkinci sıfırlama sinyali de uydu bilgisi ve menzil kodu aynı fakat taşıyıcı fazının 180º kadar sapması ile bulunur. Bu ikinci sıfırlama sinyalinin amacı alıcı tarafından alınan orijinal uydu sinyalini elimine etmektir. İkinci sıfırlama sinyali alıcının orijinal uydu sinyalini almasını engelleyerek

alıcı tarafından sadece birinci sıfırlama sinyalinin alınmasını hedefler. Sıfırlama saldırısının uygulanması zor olduğu için henüz teoride kalmıştır.



Şekil 2-10 Sıfırlama Saldırısı Blok Şeması

Sıfırlama saldırısında aldatıcı, gerçek sinyalle aynı güç gecikmesinde ancak taşıyıcı fazı ters olan sinyal gönderir. Alıcı bu sinyali aldığında, gerçek sinyalle birlikte iptal olur ve böylece alıcı gerçek sinyalin sinyal parametrelerini kaybeder ve alıcının aldatma karşıtı performansı azalır. Bu yöntemin uygulamadaki zorluğu yüksektir ve saldırı etkisi de orta-iyi seviyelerindedir.

Ortak girişim saldırısında yukarıda bahsedilen aldatma stratejisi, birden fazla aldatıcı tarafından koordine edilir. Bazı alıcılar karmaşık aldatma karşıtı yöntemler kullansalar bile, bilgilerin bütünlüğü ve güvenilirliği garanti edilemeyebilir. Bu saldırının uygulamadaki zorluğu oldukça yüksektir fakat saldırı etkisi oldukça yüksektir. Bu aldatma saldırısı referanslarda [28] numara ile belirtilmiş makalede gerçekleştirilmiş ve üç boyutlu, santimetre altı aldatma doğruluğunu başarmıştır. Fakat bu aldatma saldırısında saldırının gerçekleştirildiği çevre koşullarını da yüksek seviyede göz önünde bulundurmak gerekir.

3. ALDATMA KARŞITI YAKLAŞIMLAR

Bu bölümde aldatma karşıtı yaklaşımlar kriptografik yöntemler, anten tabanlı yöntemler, çoklu GNSS alıcı yöntemleri ve INS/IMU tabanlı yöntemler olarak dört ana başlık halinde incelenmiştir.

3.1. Kriptografik Yöntemler

Küresel Uydu Seyrüsefer Sistemlerinde (GNSS) kriptografik yöntemler, uydular ve alıcılar arasında iletilen sinyallerin ve verilerin bütünlüğünü, kimliğini doğrulamayı ve gizliliğini sağlamak için hayati bir rol oynar. Bu yöntemler, özellikle aldatma saldırılarını önlemek ve hem askeri hem de sivil uygulamalarda güvenli iletişimi sağlamak için önemlidir.

3.1.1. SAASM (Selective Availability Anti-Spoofing Module)

GPS'in tüm özelliklerine erişimi sınırlandıran ana mekanizma hem L1 hem de L2'deki P(Y) kodu yayınının şifrelenmesi olmuştur. Bu özelliğe Anti-Spoofing (AS) adı verilir. Şifrelenmiş bir P koduna P(Y) kodu denir. AS'nin temel amacı, kullanıcıyı, bir düşmanın iletmeye çalışabileceği yanıltıcı veriler içeren sahte GPS sinyallerinden korumaktır. AS, 1994'ten bu yana sürekli olarak aktiftir. Y kodlu sinyallere erişim, ABD Savunma Bakanlığı'nın yetkili kullanıcılara sunduğu şifreleme anahtarını gerektirir [3].

SPS sivil kullanıcıları L1'deki C/A kodlu sinyalle sınırlar ancak çift frekanslı ölçümler hassas konumlandırma için gereklidir. Alıcı üreticileri bu nedenle hem L1 hem de L2'deki ölçümlere erişim sağlamak için özel teknikler geliştirmiştir. Bu teknikler, aynı P(Y) kodunun her iki frekansta da bir uydu tarafından iletilmesi gerçeğinden farklı şekillerde yararlanır. Ancak, L2 ölçümleri, kodun bilinmesi durumunda olacağından çok daha kırılgan ve gürültülüdür ve çift frekanslı alıcıların maliyeti çok daha fazladır. Bu teknikler AS'yi tehlikeye atmaz çünkü Y kodlarının yapısı açığa çıkmadan kalır ve hiçbir aldatıcı sinyali üretilemez [29].

1990'lar boyunca, sınırsız kullanım için mevcut sinyaller, ölçümlere kontrollü hatalar eklenerek Seçici Kullanılabilirlik (SA) politikası kapsamında kasıtlı olarak düşürüldü. Bu hatalar, sistemin doğasında olan hatalardan önemli ölçüde daha büyüktü. SA'nın net sonucu konumlandırma hatasında yaklaşık beş kat artış oldu. Sinyal bozulması, uydu saatinin ve dolayısıyla değişen sinyaller üzerindeki zamanlama işaretlerinin

C/A kodunu, P(Y) kodunu ve taşıyıcı faz ölçümlerini eşit şekilde etkileyerek "titremesiyle" sağlandı. Seçici Kullanılabilirlik, 1 Mayıs 2000 tarihinde ABD Başkanı Bill Clinton tarafından resmi olarak kaldırıldı. Bu kararla birlikte, GPS sinyalleri sivil kullanıcılar için daha yüksek doğruluk seviyelerine ulaşmış oldu. Seçici kullanılabilirliğin kaldırılması, GPS teknolojisinin sivil uygulamalarda daha yaygın ve etkili bir şekilde kullanılmasına olanak tanımıştır.

SAASM (Selective Availability Anti-Spoofing Module), askeri kullanım için tasarlanmış özel bir GPS alıcısı modülüdür ve şifrelenmiş P(Y)-code sinyallerini ve daha sonraki versiyonları olan M-kodu sinyallerini işleyebilme kapasitesine sahiptir. Bu sinyaller, düşman etkinliklerine karşı korunmak için yüksek düzeyde gizlilik ve güvenlik sunar [3]. Sivil bir GNSS alıcısını SAASM benzeri bir alıcıya dönüştürmek mümkün olsa bile, tam bir SAASM modülünün tüm özelliklerini taklit etmek yasal olarak mümkün olmayabilir ve teknik olarak da çok zor olabilir. Ancak, bir sivil GNSS alıcısını SAASM benzeri özelliklere sahip hale getirebilmek için eklemeniz gereken özellikler aşağıda maddeler halinde belirtilmiştir.

- Şifreli Sinyal İşleme ile alıcının askeri sinyalleri dekodlayabilmesi için şifreli P(Y)-code veya M-kodu sinyallerini işleyebilme kapasitesi gerekir. Ancak, bu sinyaller yalnızca yetkili kullanıcılara açıktır.
- Anti-Spoofing teknolojisi ile sivil alıcılara, sahte sinyalleri tanıma ve gerçek sinyalleri doğrulama yeteneği kazandıracak algoritma ve teknolojiler eklenmelidir.
- Gelişmiş karıştırma karşıtı koruma ile gelişmiş sinyal işleme ve adaptif anten dizinleri kullanarak sinyal girişimine karşı koruma sağlayacak teknolojiler gerekir.
- Zamanlama ve frekans analizi ile girişim ve aldatma saldırılarını tespit etmek ve filtrelemek için zamanlama ve frekans analizi teknikleri entegre edilmelidir.
- Siber güvenlik önlemleri ile alıcının yazılım ve donanımını siber saldırılara karşı korumak için ilave güvenlik katmanları gereklidir.
- Yüksek hassasiyetli saat ile şifrelenmiş sinyallerin doğru bir şekilde işlenmesi için çok yüksek hassasiyetli ve kararlı bir saat gereklidir.
- Yüksek performanslı donanım ile yukarıdaki özellikleri desteklemek için daha güçlü işlemci ve daha gelişmiş sinyal işleme donanımı.

- Erişim kontrolü ile yalnızca yetkili kullanıcıların erişimine izin veren sıkı bir erişim kontrol sistemidir.

3.1.1.1. M-Kodu

GPS Block IIR-M uyduları ile M-kodunu destekleyen ilk uydular atılmaya başlandı. Bu uydulardan önce atılan GPS Block IIR uyduları M-kodunu desteklemiyorlardı. Eylül 2005'te atılan ilk GPS Block IIR-M uydusu ile M-kod sinyallerini destekleyen uydular atılmaya başlandı.

M-kod, mevcut sinyallerle aynı bantları paylaşmak üzere hem L1 bandında hem de L2 bandında ancak onlardan ayrı olacak şekilde tasarlandı. M-kod sinyalinde iki tepe noktasına bakıldığında taşıyıcı etrafında bölünmüş bir spektrum sinyali görülür. M-kod, P(Y) kod ve C/A kodunun merkez frekansta meydana gelen maksimum güç yoğunluklarıyla minimum örtüşme yaşar. Çünkü M-kodunun gerçek modülasyonu farklıdır. M-kodunun modülasyonu, C/A ve P(Y) sinyallerinde kullanılan ikili faz kaydırma anahtarlama (BPSK) ile farklılık gösteren ikili ofset taşıyıcı (BOC) modülasyonudur. BOC modülasyonunun bir sonucu olarak, M-kodu gücünü L1'deki P(Y) ve C/A'dan uzakta olan kenarlarda, yani boşluklarda en yüksek güç yoğunluğuna sahiptir. Bu mimari, hem uydularda ve alıcılarda uygulamayı basitleştirir hem de mevcut kodlarla girişimi azaltır. BOC modülasyon stratejisinin bu yönü, M-kodu ile eski miras sinyalleri arasında daha iyi spektral ayrım sunar.

M-kodu, askeri bir alıcı tarafından yalnızca M-kodu kullanılarak konumunu belirleyebilirken, P(Y) kodu için önce C/A kodunu edinmesi gerekiyor. Ayrıca, M-kodu 24 MHz bant genişliği üzerine yayılmıştır [30].

Bu yeni M-Kodu muhtemelen P-Kodu'nu zaman içinde değiştirecek. Bu yeni kod hem L1 hem de L2 frekanslarında taşınacak ve ABD Savunma Bakanlığı bu yeni kod ile birlikte kodun gücünü artırabilme avantajına sahip olacak. İlk olarak Y-Kodu'nun gücünü artırma fikirleri de tartışıldı fakat bu durumda C/A Kodu ile girişime uğradığı gösterildiği için bu fikirden vazgeçildi. Kısacası M-kod, L1 ve L2 frekanslarında taşınacak, ancak ikili ofset taşıyıcı modülasyonu nedeniyle eski miras kodlar olan C/A Kodu ve P-Kodu ile girişimde bulunmayacaktır [31].

GPS Sinyal Varlığı				
Taşıyıcı	Sinyal	Blok IIR	Blok IIR-M	Blok IIF
L1	P/Y	x	x	x
L2	P/Y	x	x	x
L1	CA	x	x	x
L2	L2C		x	x
L1	M		x	x
L2	M		x	x
L5	Sivil			x

Şekil 3-1 GPS Modernizasyon Sonrası Yeni Sinyaller

3.1.2. Galileo Mesaj Otantikasyonu (OSNMA)

Galileo programın kendi “Open Service” navigasyon mesajlarına kimlik doğrulama için kriptografik veri sağlayacaktır. Bu kimlik doğrulama protokolü TESLA protokolü olarak adlandırılıyor ve özellikle Galileo Open Service özel yapılmıştır [32]. Bu protokol biraz gecikme eklenerek gönderilen anahtarlar ile üretilen mesaj kimlik doğrulama kodlarını kullanır. Bu anahtar, kökü genele açık olan, kullanıcı tarafından önceden bilinen ve oluşturulmasına göre ters sırada iletilen, önceden oluşturulmuş tek yönlü bir zincirin parçasıdır. Kök anahtarın kimliği bir dijital imza (Elliptic Curve Digital Signature Algorithm) ile doğrulanır ve dijital imza genel anahtarı bir Merkle ağacı tarafından yenilenebilir. Tüm uydular için aynı anahtar zincirini kullanarak, belirli bir uydudan diğer uydular tarafından iletilen verilerin doğrulanmasına (çapraz kimlik doğrulama) olanak tanıyarak Galileo için optimize edilmiştir. Açık Hizmet Navigasyon Mesajı Kimlik Doğrulaması (Open Service Navigation Message Authentication)(OSNMA) protokol verileri, E1-B Galileo Açık Servis sinyalinde iletilen Galileo I/NAV navigasyon mesajı içerisinde iletilir. OSNMA verileri, bu belgenin yayınlandığı tarihte (2022) toplam takımyıldızdan yalnızca 20 uydu alt kümesinden iletilmektedir [33]. Geri kalan uyduların işletim sistemi verileri, OSNMA yayınlayan uydular aracılığıyla çapraz kimlik doğrulaması yapılacaktır.

OSNMA, E1 bantındaki Açık Servis Navigasyon mesajının dijital olarak imzalanmasını içerir ve TESLA (Timed Efficient Stream Loss-Tolerant Authentication) protokolünü kullanır. Bu protokol, düşük bant genişliği gereksinimleri

ve kayıp mesajlara karşı tolerans gibi avantajlara sahiptir. TESLA protokolünün ana fikri, zincirin her bir elemanının bir önceki elemandan türetilen bir anahtar zinciri kullanılarak oluşturulmasıdır. Bu, alıcının, bağımsız olarak doğrulanmış olan kök anahtar gibi bazı bilgilere sahip olmasını gerektirir [33].

OSNMA'nın çalışma prensibi, alıcının navigasyon verilerini ve düz metin navigasyon mesajını doğrulayan bir Mesaj Doğrulama Kodu'nu (MAC) demodüle etmesini, daha sonra MAC'i doğrulamak için kullanılan anahtarın sistem tarafından bir gecikmeyle yayınlanmasını ve alıcının, önceden doğrulanmış zincirdeki bir önceki anahtar veya kök anahtarla bu anahtarı doğrulamasını içerir.

Galileo OSNMA, 2020 yılında test edilmeye başlandı ve ilk testler sekiz Galileo uydusu kullanılarak yapıldı. Bu testler, daha sonra kullanıcılara konumlama ile doğrulanmış veriler sunacak işlevsel bir hizmetin ilk kanıtını oluşturdu. OSNMA'nın kamu gözlem aşaması, 2021 sonbaharında planlanmıştı ve bu aşamada OSNMA özelliklerinin, alıcı uygulama kılavuzlarının ve kriptografik anahtarların kamuoyuna açıklanması bekleniyordu.

OSNMA'nın yanı sıra, Galileo ayrıca Yüksek Doğruluk Servisi (HAS) ve Ticari Doğrulama Servisi (CAS) gibi diğer hizmetleri de sunmayı planlamaktadır. Bu hizmetler, kullanıcılara daha güvenli ve güvenilir bir uydu navigasyon deneyimi sunmak için tasarlanmıştır fakat uydu navigasyon sinyallerinin doğruluğu ve bütünlüğü garanti edilemez [34].

3.2. Anten Tabanlı Yöntemler

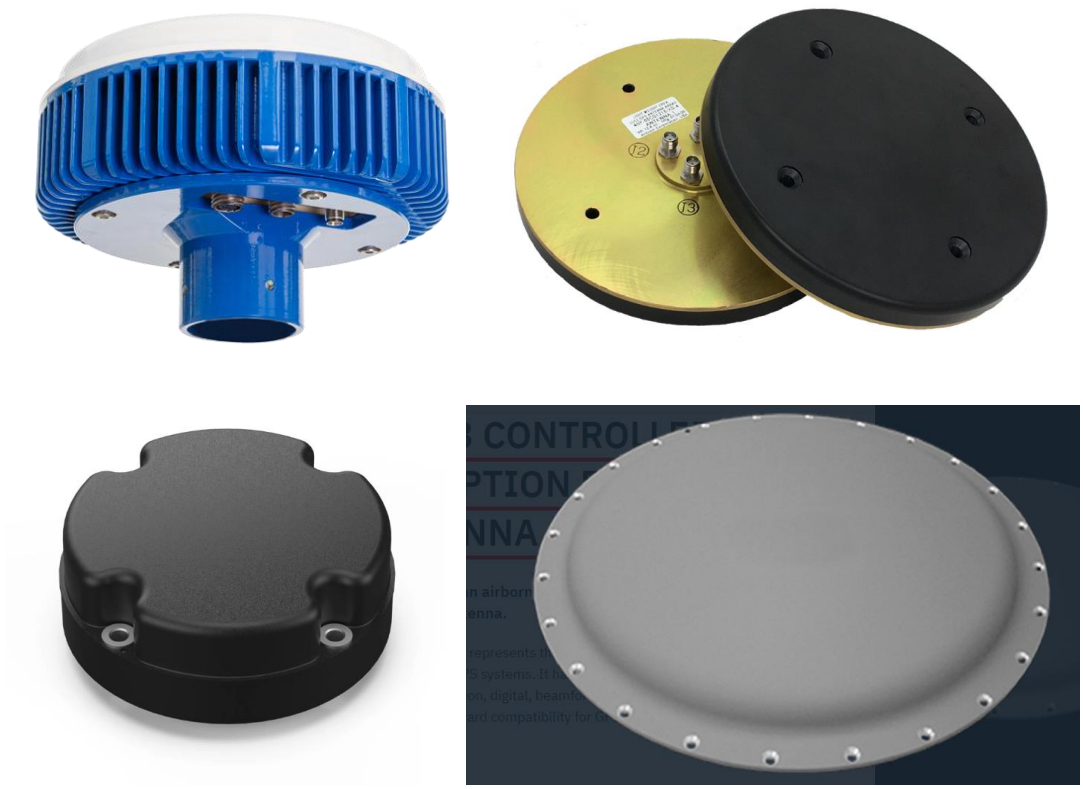
Anten dizileri, birden fazla anten elemanından oluşur ve bu elemanlar, gelen sinyalleri farklı açılardan alabilir. Bu özelliği sayesinde, anten dizileri, gelen sinyallerin yönünü ve sinyal kaynağının yerini belirlemede kullanılabilir. Gerçek GNSS uydularından gelen sinyaller, belirli bir yörüngede ve açıda olacak şekilde düzenlenmiştir. Buna karşılık, sahte sinyaller genellikle farklı yönlerden veya beklenmedik açılardan gelir. Anten dizisi teknolojisi, bu yön bilgisini kullanarak gerçek ve sahte sinyaller arasında ayrım yapabilir. Anten dizisi kullanarak gerçekleştirilen aldatma karşıtı yöntemler, sahte sinyallerin yönünü tespit ederek bu sinyalleri engelleyebilir. Örneğin, bir sahtecilik girişimi sırasında, sahte sinyal genellikle yeryüzünden veya belirli bir yönü taklit eden bir kaynaktan gelir. Anten

dizisi, bu sinyalin beklenmedik bir kaynaktan geldiğini belirleyebilir ve bu sinyali izole ederek gerçek uydu sinyallerini koruyabilir. Bu yöntem, özellikle karmaşık GNSS aldatma saldırılarına karşı etkili bir savunma sağlar. Anten dizisi temelli aldatma karşıtı yöntemler, yüksek hassasiyet ve esneklik sunar. Bu teknikler, özellikle askeri uygulamalarda, kritik altyapılar ve ticari hava taşımacılığı gibi alanlarda kullanılır. Her bir anten elemanının sinyali ayrı ayrı işleyebilme kabiliyeti, bu sistemlerin ileri seviye aldatma girişimlerine karşı daha dayanıklı olmasını sağlar. Ayrıca, bu sistemlerin gelişmiş sinyal işleme algoritmaları, çeşitli sinyal kaynaklarını analiz ederek daha güvenilir GNSS sinyalleri sağlar.

Sinyal geliş yönü (Angle of Arrival) tabanlı aldatma karşıtı yöntemi, GNSS sinyallerinin geldiği yönü tespit ederek sahte sinyalleri ayırt etmeyi amaçlar. Bu yöntem, GNSS alıcılarına entegre edilmiş birden fazla anten kullanarak çalışır ve her antenin aldığı sinyallerin zaman farklılıklarını analiz eder.

3.2.1. CRPA (Controlled Reception Pattern Antenna)

CRPA (Controlled Reception Pattern Antenna) teknolojisi, özellikle GNSS sinyalleri gibi hassas sinyal sistemlerinde kullanılan ileri düzey bir anten teknolojisidir. CRPA, jamming (sinyal bozma) ve spoofing (sahte sinyal) gibi saldırılara karşı etkili bir savunma sağlamak için tasarlanmıştır. CRPA, birden fazla anten elemanından oluşur. Bu antenler, fiziksel olarak birbirine yakın yerleştirilir, ancak Şekil 3-2'te görüldüğü gibi her biri bağımsız olarak sinyal alabilir. CRPA sistemi, gelen sinyalleri adaptif bir şekilde işler. Bu, sistem tarafından alınan sinyallerin kaynakları ve yönleri hakkında sürekli olarak bilgi toplanması ve bu bilgilere dayanarak alım deseninin (reception pattern) dinamik olarak ayarlanması anlamına gelir. CRPA, istenmeyen sinyal kaynaklarını (örneğin, jamming yapan bir kaynak veya sahte GNSS sinyalleri) tespit edebilir ve bu sinyalleri bastırabilir veya engelleyebilir. Bu, anten desenini adaptif bir şekilde ayarlayarak, istenmeyen sinyallerin etkisini azaltmak ve gerçek sinyalleri korumak için yapılır. CRPA sistemlerinde adaptif algoritmalar karıştıma kaynağının yönünü anlık olarak tespit etmekte ve dizi antenin desenini ilgili yönde sıfırlamaya (nulling) çalışmaktadır [35].



Şekil 3-2 CRPA Anten Örnekleri

3.2.2. Anten Polarizasyonu Tabanlı Yöntemler

GNSS sinyalleri, tipik olarak sağ el dairesel polarizasyonludur (RHCP). RHCP sinyallerini almak için özel olarak tasarlanmış antenler, lineer polarize veya sol el dairesel polarize gibi bu polarizasyona uymayan sinyalleri doğal olarak filtreleyebilir [3].

Bir sol el dairesel polarize (LHCP) anteni, polarizasyon uyuşmazlığı nedeniyle RHCP sinyallerine karşı genellikle duyarsızdır, bu da normal koşullar altında standart GNSS sinyallerini etkili bir şekilde almayacağı anlamına gelir. Bu da bir LCHP antenini bir aldatma/karıştırma saldırısının tespitinde kullanılma düşüncesini akıllara getirmektedir. Eğer bir LHCP anteni güçlü bir sinyal alırsa bu, özellikle sahte sinyallerin polarizasyonu doğru bir şekilde taklit etmemesi durumunda, aldatma girişimi olduğuna dair bir gösterge olabilir. Ayrıca aldatıcı, sahte sinyaller oluştururken sinyal polarizasyonunu hesaba katmayabilir ve bu şekilde de bir aldatma saldırısının tespiti yapılabilir. Bu tesbiti yapmak için LHCP anteni tarafından alınan sinyallerin güç, frekans gibi özellikleri analiz edilmesi gerekir. Ayrıca RHCP

ve LHCP antenlerinden gelen verilerin karşılaştırılması, alınan sinyallerin polarizasyonundaki farklılıkları belirleyerek tespit yeteneklerini artırır.

Bu yöntem görece basit bir aldatma karşıtı yöntemdir ve geleneksel RHCP alıcılarını aldatan saldırıları tespit ederek güvenlik katmanını artırabilir. Fakat bu yöntemde çevresel etkiler, çoklu yol yansımaları ve diğer zararsız faktörler, RHCP sinyallerinin polarizasyonunun tersine dönmesine neden olarak yanlış alarm verme gibi dezavantaja sahip olabilir. Ayrıca ileri seviyede yapılan bir aldatma saldırısında aldatıcı, bir RHCP sinyali yayınlayıp alıcıyı kandırabilir ve bu yöntem de ileri seviye tehditlere karşı etkisiz olabilir.

3.3. Çoklu GNSS Alıcı Kullanımı

GPS, GLONASS, Galileo ve BeiDou gibi birden fazla GNSS konstelasyonu kullanarak aldatmaya karşı koruma yeteneklerini artırmak, modern GNSS sistemlerinde güçlü bir yaklaşımdır. Bu strateji, farklı uydu sistemlerini kullanarak yedeklilik sağlayıp güvenliği artırırken, aldatma saldırılarına karşı da önemli bir güvenlik katmanı ekler. GNSS konstelasyonunda her sistem bağımsız olarak çalışır ve farklı uydulardan sinyaller yayınlanır. Çoklu konstelasyon sinyallerini işleyebilen alıcılar kullanarak, sistem GPS, GLONASS, Galileo ve BeiDou arasındaki konum ve zamanlama verilerini karşılıklı olarak doğrulamak iyi bir aldatma karşıtı yöntem olabilir. Çünkü bir aldatıcının farklı özellik ve geometrilerle birden fazla sistemde sahte sinyaller yayması gerekir ve bu sistemleri aldatması gerekir. Bu bir aldatıcı için iddialıdır ve bu yüzden basit aldatma teknikleri kullanmak yerine ileri seviyede bir aldatma yöntemi geliştirmesi gerekir. Bu da alıcının aldatılmasını oldukça zorlaştırır [36].

Ayrıca çoklu alıcı ile zaman ve konum verilerinin hassasiyeti artar ve herhangi bir anomalinin tespit edilmesi mümkün olur. Ek olarak bu yöntem ile bir konstelasyondaki sinyal kesilse bile diğer konstelasyondaki sinyaller ile konum rahatlıkla bulunabilir. Fakat bu yöntem diğer yöntemlere göre daha karışık ve maliyetli olabilir. Ayrıca bu sistemlerin entegrasyonu için veri füzyonu gibi yöntemler kullanılmalı ve bu şekilde konumun hesaplanması zorlaşacağından dolayı hem alıcının güç tüketimi hem de hesaplama süresi artabilir.

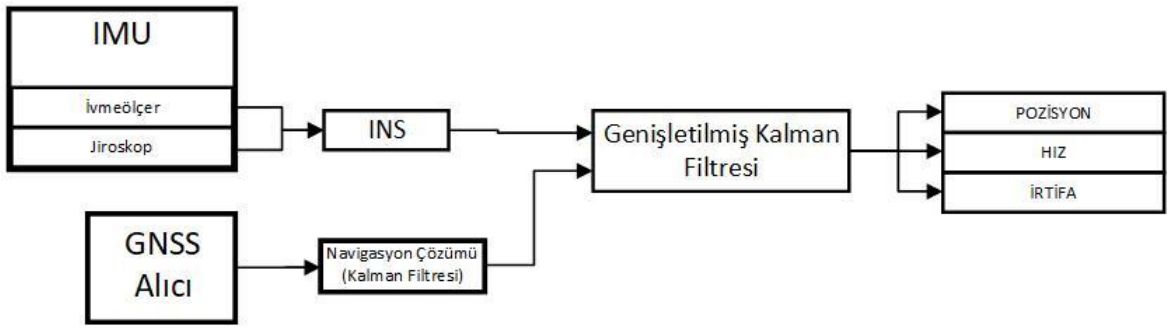
3.4. INS/IMU Tabanlı Yöntemler

GNSS sistemleri ile Ataletsel Navigasyon Sistemleri (INS) veya Ataletsel Ölçüm Birimleri (IMU) entegrasyonu, özellikle GNSS sinyallerinin tehlikeye atıldığı ortamlarda navigasyon ve konumlandırmanın güvenilirliğini ve doğruluğunu artırmak için çok etkili bir aldatma karşıtı tekniktir. Bu sistemler hızlanmaları ve açısal hızları ölçerek pozisyon, yönlendirme ve hız verileri sağlar. Bu sistemler dış sinyallere bağlı olmadığından, GNSS'yi etkileyen sahtecilik veya sinyal bozma saldırılarına karşı bağışıktırlar. Bu yüzden GNSS verileri ile INS/IMU verilerinin birleştirilmesi, GNSS sinyalleri güvenilir olmadığında veya şüpheli olduğunda bile aracın konumunun doğru bir şekilde tahmin etmeyi sağlar [37].

Bu sistemde GNSS'ten gelen veriler sürekli olarak INS/IMU sistemi tarafından sağlanan ataletsel verilerle karşılaştırılıp doğrulanabilir. GNSS tarafından türetilen pozisyonlar ile INS/IMU tarafından öngörülenler arasında önemli farklılıklar olması, muhtemel bir aldatma saldırısı olduğunu gösterir. Bu şekilde, GNSS aldatmaya karşı bir önlem olarak INS/IMU tabanlı yöntemler kullanılabilir. Ayrıca GNSS sinyallerinin engellendiği (bloklama, sinyal bozma veya aldatma nedeniyle) ortamlarda, INS/IMU geçici olarak navigasyon görevini üstlenebilir ve sürekli konum ve hız tahminleri sağlayabilir. INS/IMU sistemleri zamanla sapma gösterse de (konum ve hızda birikimli hatalar oluşsa da), kısa vadeli doğruluk genellikle çok yüksektir ve GNSS verileri tehlikeye girdiğinde boşlukları doldurabilir [38].

Bu yöntemlerin avantajları arasında GNSS sinyalleri tehlikeye girdiğinde, INS/IMU verileri bilgi kaynağı olarak yedek veya tamamlayıcı olarak kullanılarak navigasyonun güvenilirliğinin artırılması söylenebilir. GNSS ve INS/IMU verilerinin birleştirilmesi, bir sistemdeki hataların diğerinin güçlü yönleriyle telafi edilmesiyle daha yüksek genel doğruluk sağlar. INS/IMU, GNSS verilerinin geçerliliğini kontrol ederek güvenlik katmanı ekler. Fakat dezavantaj olarak GNSS ve INS/IMU sistemlerini birbirine entegre etmek navigasyon sistemlerinin karmaşıklığını ve maliyetini artırır. Ayrıca zamanla INS/IMU sistemleri, özellikle GNSS düzeltmeleri olmadan sapma yaşar. Bu durumu yönetmek için düzenli kalibrasyon ve ileri seviyede sensör füzyon algoritmaları gereklidir. Bu yüzden iki sistemin entegrasyonu için teknikler geliştirilmiştir. En yaygın kullanılanları gevşek bağlantılı ve sıkı bağlantılı entegrasyonlardır [39].

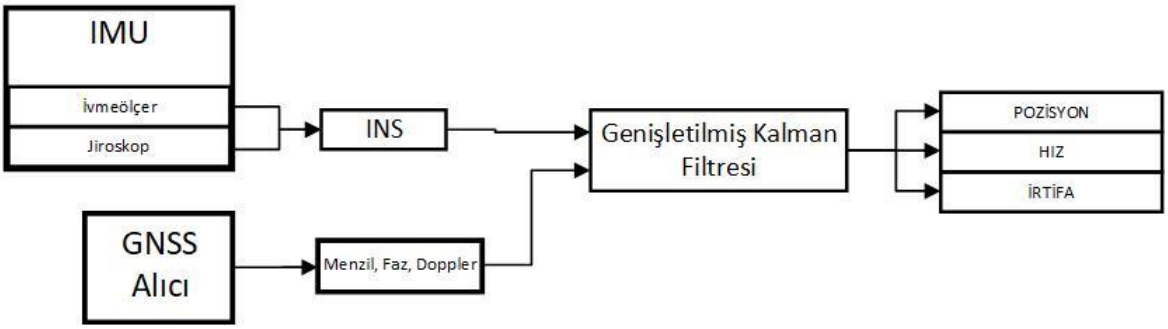
Bu entegrasyon yöntemlerini inceleyecek olursak gevşek bağlantılı şemada, INS doğrudan GNSS navigasyon çıktılarıyla (pozisyon, hız) genellikle bir Genişletilmiş Kalman Filtresi kullanılarak birleştirilir. INS integrasyon hataları, GNSS pozisyon girdileri ile düzeltilir ve Kalman filtresi tarafından kararlı navigasyon çıktıları sağlanır. Bu yöntem basitlik açısından büyük bir avantaja sahiptir. Ayrıca sınırlı hesaplama gücüne sahip minyatür cihazlarda çalıştırılabilir. Ek olarak, SAASM (askeri) veya standart NMEA protokolünü kullanan üçüncü taraf cihazlarla entegrasyon için de en iyi çözümdür [40]. Bu yöntemin blok şeması Şekil 3-3 'te gösterilmiştir.



Şekil 3-3 Gevşek Bağlı GNSS/INS Entegrasyonu

Sıkı bağlı entegrasyon ise daha karmaşık bir yöntemdir. Bu şemada GNSS alıcısı sadece ham ölçümleri hesaplar ve görülen her uydu ile ilgili çeşitli pozisyon ölçümleri sağlar. GNSS alıcısı herhangi bir navigasyon filtresi çalıştırmaz. Tüm GNSS denklemleri doğrudan INS/GNSS Genişletilmiş Kalman filtresine entegre edilir.

Bu tür bir entegrasyonun en büyük avantajı, bireysel uydulardan hatalı ölçümleri belirleme veya geçici olarak sınırlı sayıda uydu ile çalışabilme (<4) yeteneğini önemli ölçüde artırmasıdır. Bu, sıkı bağlantılı çözümün gevşek bağlantılı entegrasyona kıyasla mükemmel bir dayanıklılık sağlamasına olanak tanır. Yüksek hassasiyetli uygulamalarda (Real Time Kinematic) sıkı bağlantı, kesintiden sonra RTK düzeltme kurtarma süresini hızlandırarak santimetre seviyesinde doğruluk elde etme imkanını artırır. Sıkı bağlantının ana sınırlaması, genellikle ham ölçümleri sağlamayan harici GNSS alıcılarla kolayca entegre edilememesidir. Bu yöntemin blok şeması Şekil 3-4 'te gösterilmiştir.



Şekil 3-4 Sıkı Bağlı GNSS/INS Entegrasyonu

4. ALDATMA KARŞITI ALMAÇ MİMARİSİ

Bu çalışmada birçok aldatma yöntemine değinilmiştir. Bu aldatma yöntemleri ayrı ayrı incelendiğinde o kadar zararlı gözükmeseler de birçok aldatma tekniğinin ardı ardına uygulanarak gerçekleştirildiği aldatma saldırıları oldukça tehlikeli olmaktadır. Bu yüzden aldatma karşıtı bir mimari belirlerken birçok aldatma saldırısına karşı dayanıklı, farklı aldatma senaryolarında etkili bir mimari geliştirmemiz gerekir.

Nasıl ki birçok aldatma yöntemi bulunmakta ise bunlara karşılık gelen birçok aldatma karşıtı karşı tedbir bulunmaktadır. Bütün aldatma saldırılarına tek bir karşı tedbir olmadığı için birçok aldatma karşı tedbirini bir almaç içinde barındırmamız gerekir. Bu yüzden birçok aldatma karşı tedbirini içeren bir GNSS alıcısı mimarisini sunmak gerekir. Bu nedenle, önerdiğimiz mimaride, çoklu konstelasyon destekleyen GNSS alıcısı, CRPA anteni ve ivmeölçer sensörü ile donatılacaktır. Alıcıdan ve sensörden gelen veriler, veri füzyonu yöntemleriyle birleştirilerek aldatma tespiti yapmak amaçlanmaktadır. Esasen bu mimaride, mevcut sivil bir GNSS alıcısına takılan bir aldatma dedektörü ile aldatma tespiti yapılabilecektir. Bu aldatma dedektörü ilerleyen paragraflarda anlatılan parametrelere bakarak aldatma tespiti yapabilir.

İlk olarak herhangi bir nesnenin yapabileceği hız sınırlıdır. Yani bir kara aracının, bir hava aracının ve bir deniz aracının farklı değerlerde maksimum yapabileceği bir hız sınırı vardır. GNSS alıcısı da x, y ve z eksenlerinde hız verisi sağlar. GNSS alıcısından sağlanan bu hız verisinin büyüklüğü, alıcının takıldığı platformun hız sınırını aşmaması gerekir. Başka bir deyişle;

$$\sqrt{V_x^2 + V_x^2 + V_x^2} = |V| \tag{1}$$

$$V_{min} < V_{GNSS} < V_{max} \tag{2}$$

IMU sensörleri, INS/IMU tabanlı aldatma karşıtı yöntemler başlığında anlatıldığı gibi x, y, z eksenlerinde ivmelenme (accelerometer) verisini verirler. Bu mimaride bir ivmelenme verisi veren bir IMU sensörü kullanılabilir. Bir IMU sensörü yerine bir ivmeölçer sensörü kullanılabilir. Bu ivmelenme verisi, herhangi bir nesne için belli bir değerin üzerinde olamayacağı gibi bir kara aracında, bir hava aracında ve bir deniz aracında farklı değerlerde bir maksimum değeri vardır. IMU sensörü ile elde edilen x, y, z eksenlerinde ivmelenme verisinin büyüklüğü aşağıdaki şekilde bulunur.

$$\sqrt{a_x^2 + a_y^2 + a_z^2} - 9{,}8 = |a| \tag{3}$$

$$a_{min} < a_{IMU} < a_{max} \tag{4}$$

Ayrıca GNSS alıcısından aldığımız hız verisinin zamana göre türevini alırsak aynı şekilde ivmelenmeyi elde ederiz.

$$a(t) = \frac{dv(t)}{dt} \tag{5}$$

(1) denkleminde belirtildiği gibi hız verilerinin büyüklüğü alınıp zamana göre nümerik olarak türevleri alınırsa ivmelenme verisi elde edilir ve bu veri ile IMU sensöründen gelen ivmelenme verilerinin uyumlu olması beklenir. Matematiksel olarak ifade etmek gerekirse;

$$\sqrt{(|a_{GNSS}| - |a_{IMU}|)^2} \leq \Delta a \text{ veya} \tag{6}$$

$$\big||a_{GNSS}| - |a_{IMU}|\big| \leq \Delta a \tag{7}$$

Ek olarak IMU sensöründen alınan ivmelenme verilerinin nümerik olarak integrali alınarak hız verilerine ulaşılabilir.

$$v(t) = \int a(t)dt + v_0 \tag{8}$$

Aynı şekilde burada elde edilen hız verileri ile GNSS alıcısından elde edilen hız verilerinin de birbiriyle uyumlu olması gerekir. Diğer bir deyişle;

$$\sqrt{(|v_{GNSS}| - |v_{IMU}|)^2} \leq \Delta v \text{ veya} \tag{9}$$

$$\big||v_{GNSS}| - |v_{IMU}|\big| \leq \Delta v \tag{10}$$

Ayrıca GNSS alıcısının verdiği konum çözümü üzerinde de bir sınırlama getirilip bu sınırlama ile aldatma tesbiti yapılabilir. Çünkü her platformun maksimum bir yer değiştirmesi olur. Bu yer değiştirme verisi eğer platform sınırlarını aşacak şekilde gelirse de bir aldatma saldırısı olduğu tesbit edilebilir.

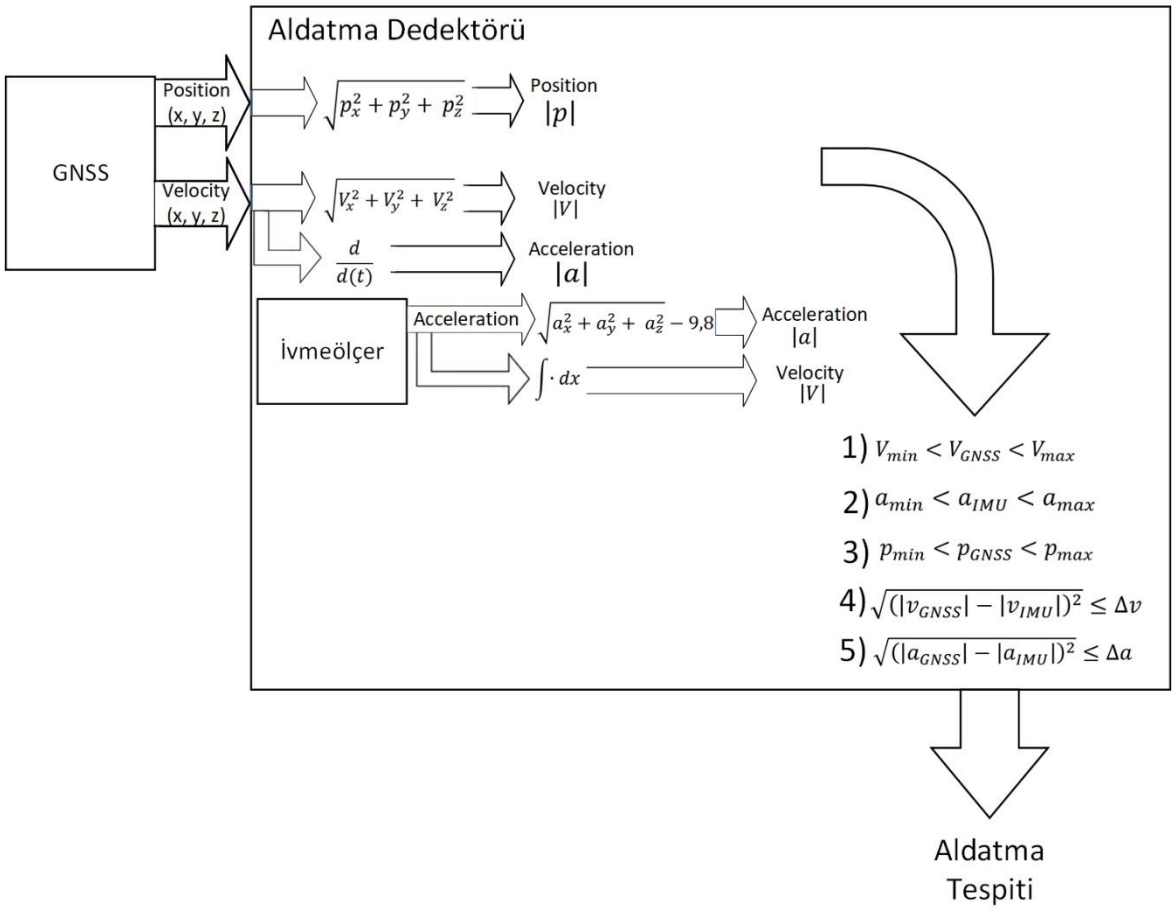
$$\sqrt{p_x^2 + p_y^2 + p_z^2} = |p| \tag{11}$$

$$p_{min} < p_{GNSS} < p_{max} \tag{12}$$

Belirtilen maddeler ile oluşturulan aldatma dedektörünün blok şeması Şekil 4-1 gösterilmiştir. Bu blok şemada yukarıda anlatıldığı gibi GNSS alıcısından ve

ivmeölçer sensöründen elde edilen verilerin işelenip bir aldatma saldırısının varlığı tespit edilmeye çalışılmıştır.

Yukarıda belirtilen maddeleri sivil bir GNSS alıcısına eklediğimizde birçok aldatma metodunu elimine edecek bir aldatma karşıtı mimari elde edilmiş olur. Buna ek olarak CRPA antenini de sivil bir GNSS alıcıya entegre ettiğimizde bu antenin karıştıma önleyici yapısı ve belli bir güç seviyesinin üstündeki sinyalleri izole etmesi bu GNSS sistemini aldatmalara karşı korunaklı yapar.



Şekil 4-1 Aldatma Dedektörü Blok Şeması

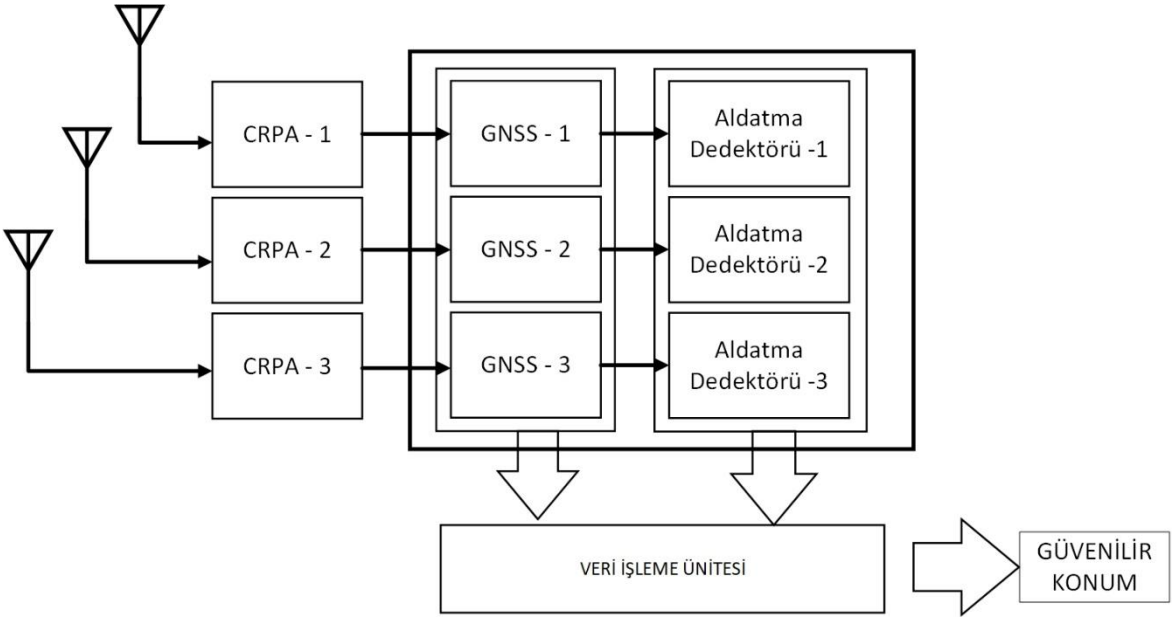
İvmeölçer sensörü ve CRPA antenini içeren önerilen GNSS aldatma karşıtı alıcı mimarisi, aldatma saldırılarına karşı sağlam bir savunma sunar. CRPA anteninin gelişmiş mekansal filtreleme ve null steering yetenekleri, alım deseninin dinamik olarak ayarlamasına olanak tanıyarak aldatma sinyallerini etkili bir şekilde izole eder ve etkisiz hale getirir. Bu uyarlanabilir yanıt, yalnızca gerçek GNSS sinyallerinin

işlenmesini sağlar ve karmaşık aldatma girişimlerine rağmen konumlandırma bilgilerinin bütünlüğünü korur. CRPA anteninin sağladığı mekansal çeşitlilikten yararlanarak sistem, gelen sinyallerin yönünü ayırt edebilir ve beklenen desenlerden sapma gösterenleri reddedebilir.

Buna ek olarak, ivmeölçer sensörünün entegrasyonu, GNSS sinyalleriyle çapraz referans yapılabilecek bağımsız hareket verileri sağlayarak alıcıya kritik bir güvenlik katmanı ekler. Bu sensör, alıcının hareketini sürekli olarak izler ve ivmeölçer verileri ile GNSS'ten türetilen veriler arasındaki herhangi bir tutarsızlık anında bir aldatma girişimini işaret eder. İvmeölçer sensörünün yüksek frekanslı hareket güncellemeleri, gerçek zamanlı doğrulama sağlar ve hareketlerdeki hızlı değişikliklerin bile doğru bir şekilde izlenip doğrulanmasını garanti eder. Bu yedeklilik, GNSS sinyalleri tehlikeye girse bile sistemin güvenilir ve doğru kalmasını sağlar. Daha yüksek güvenilirlik içinse birden çok GNSS alıcısı, CRPA anteni ve aldatma dedektörü olan bir sistem yapılıp verilerin işlenerek Şekil 4-2’de görüldüğü gibi doğru ve güvenilir pozisyon çözümü elde edilir.

Şekil 4-2’de görüldüğü gibi en az 3 tane GNSS alcısı, CRPA anteni ve aldatma dedektörü sistemini birleştirip bu sistemlerden gelen konum ve aldatma verilerini bir veri işleme ünitesinde birleştirirsek ve aldatma olan sistemden gelen konum verisini yoksayıp aldatma olmayan sistemden gelen konumları karşılıklı olarak kontrol edip doğru konumu bulmamızı sağlar.

CRPA anteni ve ivmeölçer sensörünün yanı sıra farklı sistemlerden gelen verilerin işlenmesi ve bu sistemlerin karşılıklı olarak kontrol edilmesi sistemi aldatmaya karşı neredeyse tam güvenilir hale getirir. Çoklu sensör yaklaşımı, GNSS verilerindeki herhangi bir anormalliğin hızla tespit edilmesini ve hafifletilmesini sağlayarak güvenilir bir navigasyon çözümü sunar. Bu mimari, GNSS güvenliğinde önemli bir ilerlemeyi temsil eder ve kesin ve güvenilir konumlandırma bilgilerine dayanan kritik uygulamalar için geliştirilmiş koruma sağlar.



Şekil 4-2 Sistem Blok Şeması

5. DENEYSEL ÇALIŞMALAR

Deneysel çalışmalar kapsamında ilk olarak deneysel çalışmalarda kullanılan cihazlardan ve bunların teknik özelliklerinden bahsedilip, ardından bir aldatıcı kurulumu yapılmıştır. Son olarakta aldatma karşıtı önlemler ile ilgili deneysel çalışmalar yapılıp sonuçlar bölümüne geçilmiştir.

5.1. Çalışmalarda Kullanılan Cihazlar

Bu başlık altında, deneysel çalışmalarda kullanılan GNSS simülatörü, GNSS alıcı, GNSS alıcı arayüzü, sinyal üreteçleri ve antenlerin teknik özellikleri ele alınmıştır.

5.1.1. USRP

USRP (Universal Software Radio Peripheral), geniş bir radyo iletişimi deneyleri ve uygulamaları yelpazesini mümkün kılmak için tasarlanmış bir tür Yazılım Tanımlı Radyo (SDR) donanımıdır. Hem akademik hem de endüstriyel araştırmalarda yaygın olarak kullanılan ve kablosuz sinyallerle ilgili pratik uygulamalarda kullanılan çok yönlü bir araçtır.

USRP cihazları, radyo frekansı (RF) iletişimlerinin incelenmesini ve uygulanmasını kolaylaştırmak için tasarlanmıştır. Bilgisayardaki dijital sinyalleri antenler aracılığıyla iletilebilen ve alınabilen analog sinyallere dönüştürerek, yazılım uygulamaları ile radyo dalgalarının fiziksel dünyası arasında bir köprü görevi görür.

Mimari ve bileşenleriden bahsetmek gerekirse RF önyüzü, gelen ve giden RF sinyallerini işleyen yükselteçler, filtreler ve karıştırıcıları içerir. Bu bileşen, zayıf sinyalleri güçlendirerek veya giden sinyalleri iletime hazırlayarak bu sinyalleri düzenlemekten sorumludur.

Üzerinde bulunan yerel osilatör bileşeni, gelen ve giden sinyallerle karışarak radyo iletişimleri için gerekli frekans çevirisini sağlamak üzere kullanılan sabit bir frekans üretir.

Ayrıca üzerinde FPGA (Alan Programlanabilir Kapı Dizisi) bulunmaktadır. FPGA, gerçek zamanlı dijital sinyal işleme görevlerini gerçekleştirebilen son derece esnek

ve programlanabilir bir çiptir. Filtreleme, modülasyon ve demodülasyon gibi çeşitli dijital sinyal işleme görevlerini yerine getirebilir.

Arayüz olarak USRP'ler; USB, Ethernet veya PCIe gibi arayüzler aracılığıyla ana bilgisayara bağlanır. Bu bağlantılar, dijitalleştirilmiş radyo sinyallerini, USRP donanımı ile bilgisayarda çalışan yazılım arasında taşır.

İşlevsellik ve kabiliyetlerinden bahsetmek gerekirse frekans aralığı birkaç kHz'den birkaç GHz'e kadar geniş bir frekans aralığını kapsayabilir ve bu da onları FM radyo, TV yayını, hücresel iletişimler ve uydu sinyalleri gibi birçok farklı uygulama için uygun hale getirir. AM, FM, QAM, PSK ve daha fazlası gibi çeşitli modülasyon şemalarını desteklerler. Bu, USRP'leri, işleyebilecekleri iletişim türleri açısından son derece esnek hale getirir.

Bu cihazlar yazılım uyumluluğu bakımından GNU Radio ve LabVIEW programları ile kullanılabilirler. GNU Radio, USRP ile en sık kullanılan yazılım çerçevelerinden biridir. GNU Radio, kullanıcıların karmaşık radyo iletişim sistemlerini tasarlayıp simüle edebilecekleri geniş bir sinyal işleme bloğu kitaplığı ve grafiksel bir arayüz (GRC - GNU Radio Companion) sağlar. LabVIEW, özellikle akademik ve araştırma ortamlarında popüler bir diğer araçtır ve USRP ile özelleştirilmiş SDR uygulamaları geliştirmek için kullanılır. Görsel bir programlama yaklaşımı sunar ve gerçek zamanlı veri işleme görevlerini yönetmek için uygundur.

USRP cihazları, sınıflarda basit eğitim araçlarından, kablosuz iletişim teknolojileri, radar sistemleri, kablosuz ağ tasarımı, sinyal istihbaratı gibi birçok araştırma projelerinde ve çeşitli uygulamalarda kullanılır.

Bu deneysel çalışmalarda kullanılan NI USRP-2901 cihazının TX hattının ve RX hattının teknik özellkleri sırasıyla Çizelge 5.1 ve Çizelge 5.2 de verilmiştir [41].

Çizelge 5.1 - USRP TX hattının özellikleri

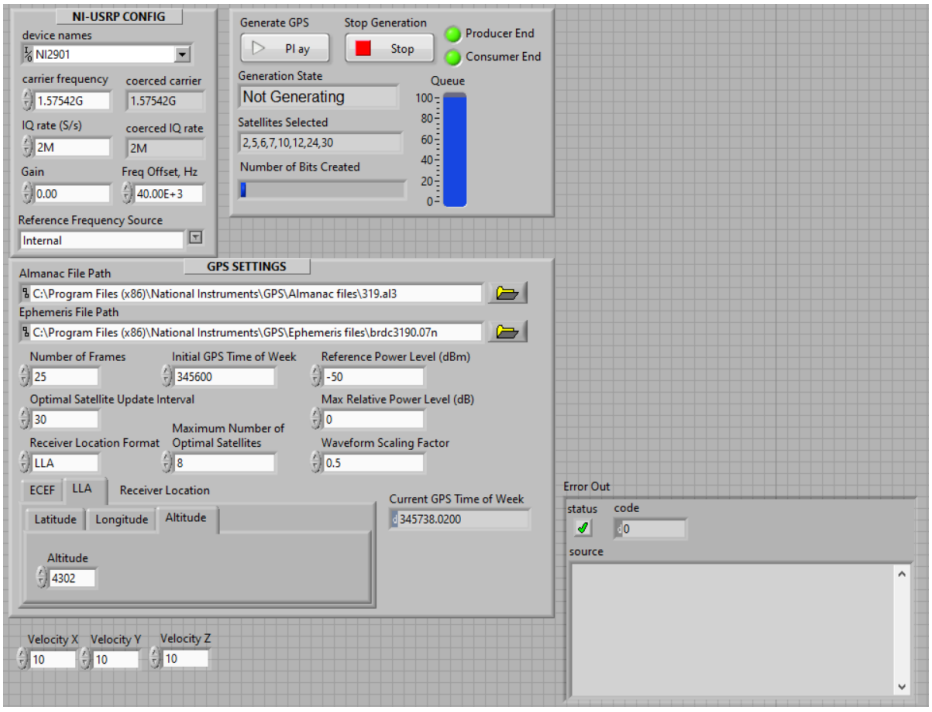
Frekans Aralığı	70 MHz - 6 GHz
Frekans Adımı	<1 kHz
Maksimum çıkış gücü(P_{out})	20 dBm
Kazanç aralığı	89.75 dB
Kazanç adımı	0.25 dB
Frekans doğuluğu	2.5 ppm
Maksimum anlık gerçek zamanlı bant genişliği	56 MHz
Akış	15 MS/s (Maksimum I/Q oranı)

Çizelge 5.2 - USRP RX hattının özellikleri

Frekans Aralığı	70 MHz - 6 GHz
Frekans Adımı	<1 kHz
Kazanç aralığı	76 dB
Kazanç adımı	1.0 dB
Maximum giriş gücü(P_{in})	-15 dBm
Gürültü Tabanı	5 dB to 7 dB
Frekans doğruluğu	2.5 ppm
Maksimum anlık gerçek zamanlı bant genişliği	56 MHz
Akış	15 MS/s (Maksimum I/Q oranı)
Sayısal – Analog Çevirici	12 bit (Maksimum I/Q oranı)

Şekil 5-1 NI USRP 2901

USRP cihazları çeşitli şekillerde programlanabilirler. Bu yöntemlerinden biri GNU Radio programı kullanılarak USRP cihazını programlamaktır fakat bu yöntemi uygulamak için USRP cihazının içindeki bellenimin yerine farklı bir bellenim yüklemek gerekmektedir. Bu yüzden bu çalışmada diğer programlama yöntemi olan USRP cihazında bulunan bellenim ile Labview programı kullanılarak USRP cihazı kontrol edilmiştir. Bu kontrolün sağlanması için gerekli Labview lisansları yüklenmiş (GPS/GNSS toolbox) ve bu lisanslar ile program geliştirilmiştir.



Şekil 5-2 GPS Simülatör Uygulaması

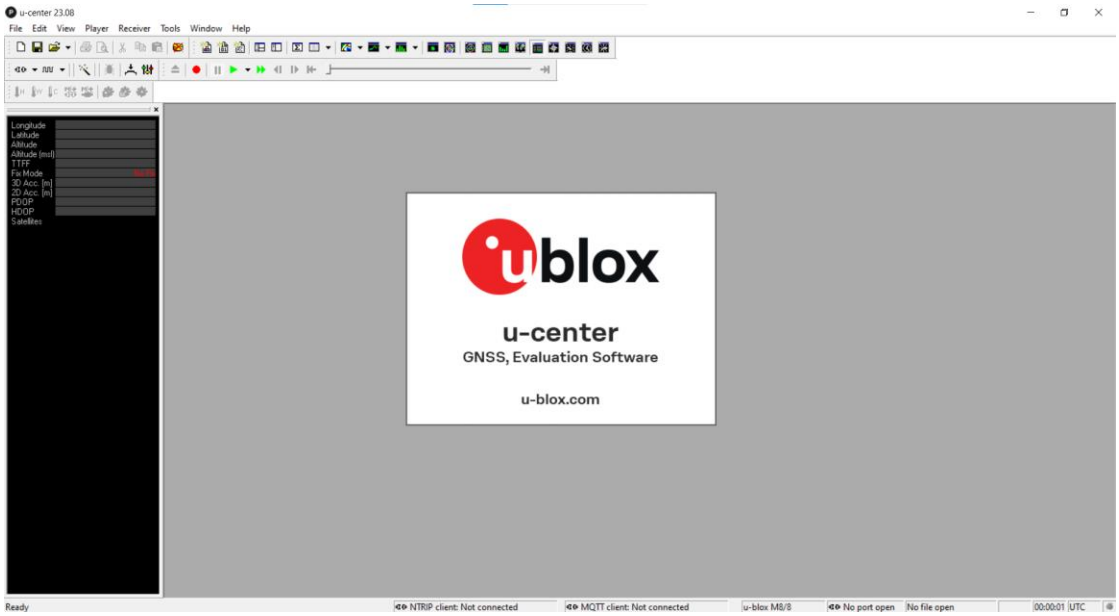
Geliştirilmiş olan Labview yazılımının arayüzü Şekil 5-2 de verilmiştir. Şekil 5-2'de görüldüğü gibi taşıyıcı frekansı GHz cinsinden ve kazanç dB cinsinden ayarlanabilir olarak bulunmaktadır. Ayrıca istenildiği takdirde dışarıdan bir frekans kaynağı ile referans verilebilmektedir. Almanac ve efemeris verileri seçilebilir ve istenildiği takdirde geçmiş veya gelecekteki bir tarihteki veriler girilebilir. Burada bölüm (Frame) sayısı GPS bölüm (frame) sayısını ifade eder. Herbir bölüm 5 tane alt bölümden oluşur. Herbir alt bölüm ise 30 bitten oluşan 10 adet kelime içerir. Yani toplamda herbir bölüm 10*5*30 = 1500 bitten oluşur. Sonuç olarak bölüm sayısı 25 olarak belirlenirse 25*1500 = 37500 bit sayısı olur. Bu da 1 saniyede 50 bit hızı ile hesaplanacak olursa toplamda 12.5 dakikalık bir zaman dilimine denk gelir.

5.1.2. u-center Programı

u-center, u-blox şirketi tarafından GNSS (Küresel Navigasyon Uydu Sistemi) alıcılarını değerlendirmek, yapılandırmak ve test etmek için geliştirilen güçlü ve çok yönlü bir yazılım aracıdır. Öncelikli olarak u-blox'un GNSS modülleri ve çipleri ile kullanılmak üzere tasarlanmıştır, ancak diğer GNSS cihazlarıyla da çalışabilir. Bu arayüz ile alıcının pozisyonu, hızı ve zamanı (PVT) hakkında gerçek zamanlı bilgi gösterir, izlenen uydular hakkında sinyal gücü, uydu kimliği ve pozisyon gibi detayları gösterir.

Kullanıcıların GNSS verilerini daha sonra analiz etmek üzere kaydetmelerini sağlar. Kayıtlar ham veri, NMEA cümleleri ve u-blox'a özgü mesajları içerebilir. Ayrıca kullanıcılar, kaydedilen verileri detaylı analiz ve sorun giderme için tekrar oynatabilir.

GNSS alıcı ayarlarını yapılandırmak için bir arayüz sağlar. Kullanıcılar güncelleme hızı, güç modları ve iletişim protokolleri gibi ayarları bu arayüz aracılığıyla kolay bir şekilde yapabilir. Kullanıcıların alıcıdan hangi NMEA veya u-blox'a özgü mesajların çıkış yapılacağını seçmelerine olanak tanır.



Şekil 5-3 u-center Programı

5.1.3. u-blox C099-F9P Uygulama Kartı

u-blox C099-F9P Application Board, deneysel çalışmalarda kullanılan, üzerinde ZED-F9P-04B GNSS alıcısı ve ODIN-W260 multiradio modülü (Bluetooth, Wi-Fi) bulunan USB arayüzü ile kolayca bilgisayara bağlanıp u-center programı ile kontrol edilebilen bir geliştirme kartıdır.

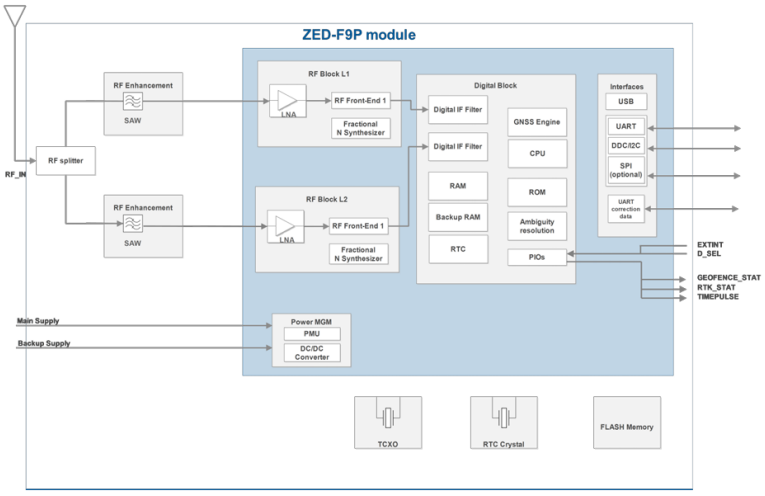
Üzerinde bulunan ZED-F9P-04B GNSS alıcısı hakkında bilgi vermek gerekirse ZED-F9P-04B konumlandırma modülü, yüksek hacimli endüstriyel uygulamalar için çok bantlı GNSS sağlayan u-blox F9 alıcı platformunu kullanır. ZED-F9P-04B, santimetre seviyesinde doğruluk için entegre u-blox çok bantlı RTK ve PPP-RTK1 teknolojilerine sahiptir. Bu modül birden fazla GNSS konstelasyonunu (constellation) alıp izleyebilen eşzamanlı GNSS alıcılarından oluşur. Çok bantlı RF ön yüzü mimarisi sayesinde, GPS, GLONASS, Galileo ve BeiDou gibi dört ana GNSS konstelasyonu ile birlikte SBAS ve QZSS uyduları da eşzamanlı olarak alınabilir. Bu modülün desteklediği sinyaller aşağıdaki Çizelge 5.3'te verimiştir.

Çizelge 5.3 - ZED-F9P-04B GNSS alıcısını desteklediği sinyaler

GPS / QZSS	GLONASS	Galileo	BeiDou
L1C/A (1575.420 MHz)	L1OF (1602 MHz + k*562.5 kHz, k = –7,..,6)	E1-B/C (1575.420 MHz)	B1I (1561.098) MHz
L2C (1227.600 MHz)	L2OF (1246 MHz + k*437.5 kHz, k = –7,..,6)	E5b (1207.140 MHz)	B2I (1207.140 MHz)

Ayrıca kullanılan GNSS modülünün blok şeması (Şekil 5-5) ve u-blox C099-F9P uygulama kartının görseli Şekil 5-4 te gösterilmiştir [42].

Şekil 5-4 u-blox C099-F9P Application Board



Şekil 5-5 ZED-F9P-04B Modülü Blok Şeması

5.1.4. Anritsu MG36221A Sinyal Üreteci

MG3690C serisi RF/Mikrodalga sinyal jeneratörleri, ses, HF, VHF, UHF ve RF frekanslarını kapsar ve tek bir koaksiyel çıkışla 9 kHz – 20 GHz frekans bantlarında sinyal sağlar. Düşük faz gürültüsü, hızlı anahtarlama ve yüksek performanslı darbe modülasyonu dahil olmak üzere geniş bir analog modülasyon yelpazesi sunar. Kablosuz iletişim, havacılık ve savunma, tüketici ve bilgisayar elektroniği gibi çeşitli endüstriler için bileşen ve sistemlerin tasarımı ve test edilmesi için bir sinyal kaynağı çözümü olabilecek bir cihazdır. Bu cihazın RF özellikleri Çizelge 5.4 te gösterilmiştir.

Çizelge 5.4 - Anritsu MG36221A RF özellikleri

Parametre	Teknik Özellik
Frekans Aralığı	2 GHz – 20 GHz
Frekans Çözünürlüğü	0.01 Hz
Frekans Anahtarlaması	2 mSec min
Referans Çıkış Frekansı	10 MHz, 1V pk-pk @ 50 Ohms
Çıkış Gücü	-120 dBm to +19 dBm (< 40 GHz çıkış) -120 dBm to +13 dBm (> 40 GHz, < 50 GHz) -120 dBm to +3 dBm (> 50 GHz, <67 GHz)
Seviye doğruluğu	± 1dB (< 40GHz çıkış) ± 1.5 dB (< 67 GHz çıkış)
SSB Gürültü Seviyesi	-119 dB/Hz (typ) @ 10 GHz çıkış, 10 KHz offset
Harmonik (2 GHz to 20 GHz)	-60 dBc

Bu cihazın modülasyon yetenekleri de Çizelge 5.5'te gösterilmiştir.

Çizelge 5.5 - Anritsu MG36221A modülasyon özellikleri

Parametre	Teknik Özellik
FM sapma max	± 100 MHz
PM sapma max	400 rad (Geniş Modda)
AM Bant Genişliği	DC to 100 KHz
AM Derinliği	0% to 90%
Pulse Modülasyonu On/Off Oranı	80 dB
Pulse Modülasyonu Rise/Fall Zamanı	5 ns (typ)
Pulse Genişliği (min)	< 10 ns (Düzenlenmemiş)

Ayrıca MG36221A cihazı frekans tarama özelliği de bulunmaktadır. Bu özelliklerinin detayları da Çizelge 5.6'da verilmiştir.

Çizelge 5.6 - Anritsu MG36221A frekans tarama özellikleri

Parametre	Teknik Özelliği
Frekans Tarama Çalışma Modları	Adım, Liste ve Rampa
Frekans Tarama Genişliği	0.01 Hz - bütün frekans bandı (Adım, Liste Modlarında) 1 MHz – bütün frekans bandı (Rampa Modunda)
Power Sweep Operating Modes	Adım
Power Sweep Resolution	0.01 dB/adım

Şekil 5-6 Anritsu MG36221A Cihazı

5.1.5. TTI TGR2050 Sinyal Üreteci

2 GHz frekansa ve 7 dBm güce kadar sinyal üretebilen bu sinyal üretecinin teknik özellikleri Çizelge 5.7'de verilmiştir.

Çizelge 5.7 - TTi TGR2050 sinyal üreteci teknik özellikleri

Parametre	Teknik Özellik
Frekans	150 kHz - 2000MHz
Çıkış Seviyesi	-127dBm - +7dBm
Çıkış Seviyesi Doğrulğu	±2dBm
Harmonikleri	<-25dBc@+7dBm.
Çıkış Tipi	Çıkış Empedansı 50,Type N konnektör.

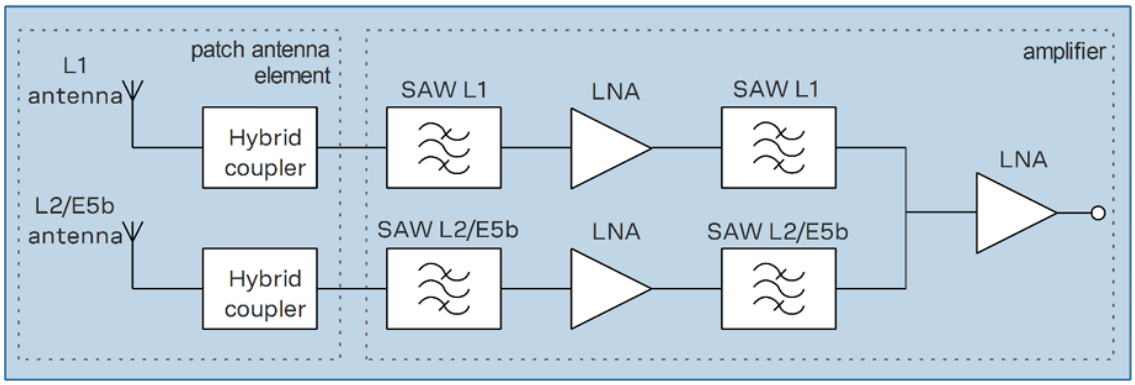
Şekil 5-7 TTI TGR2050 Sinyal Üreteci

5.1.6. Antenler

Deneysel çalışmalar kısmında çeşitli antenler kullanılmıştır. Bu antenlerden ilki u-blox markasının Ann-Mb-00 anteni, ikincisi ANDPROG markasının GGB236 anteni ve sonuncusu ise TUALCOM markasının TUALAJ-4300-D antenidir.

5.1.6.1. Ann-Mb-00-00 Anteni

Bu anten çok bantlı (L1, L2/E5b/B2I), yüksek doğruluk veren bir aktif GNSS anteni olarak geçer. Bu yüksek performanslı, çok bantlı, sağ el dairesel polarize (RHCP), çift beslemeli patch anten elemanı, dahili yüksek kazançlı LNA (düşük gürültülü güç yükselteci) ile SAW (Surface Acoustic Wave) ön filtreleme sunar. Antenin blok şeması aşağıdaki görselde gösterilmiştir [43].



Şekil 5-8 Ann-Mb-00-00 Anteni Blok Şeması

Ayrıca antenin ve antenin içinde bulunan düşük gürültülü güç yükseltecinin parametreleri Çizelge 5.8 ve Çizelge 5.9'da verilmiştir [44].

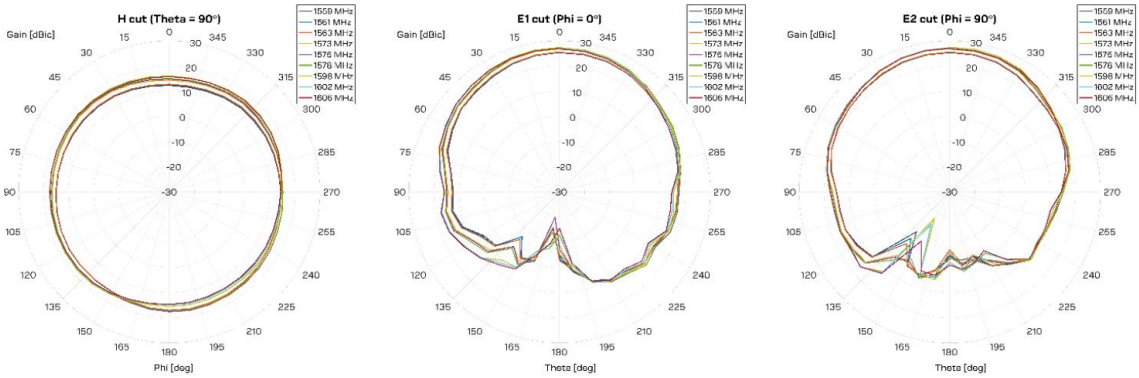
Çizelge 5.8 - Anten parametreleri

Parametre	L1 Bandı	L2/E5b/B2I Bandı
Frekans	1559-1606 MHz	1197-1249 MHz
Empedans	50 Ω	50 Ω
Kazanç	Typ. 3.5 dBic (Zenith)	Typ. 0.0-2.0 dBic (Zenith
Polarizasyon	RHCP	RHCP
Axial oran	Max. 2.0 dB (Zenith)	Max. 2.0 dB (Zenith)

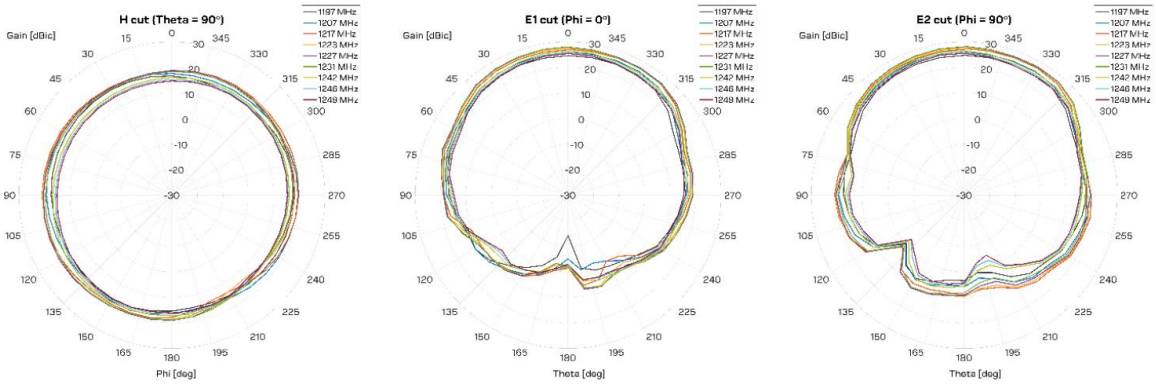
Çizelge 5.9 - Düşük gürültülü güç yükselteci parametreleri

Parametre	L1 Bandı	L2/E5b/B2I Bandı
Frekans	1559-1606 MHz	1197-1249 MHz
Empedans	50 Ω	50 Ω
LNA Kazancı	Typ. 28 ± 3.0 dB	Typ. 28 ± 3.0 dB
Gürültü Şekli	Max. 2.8 dB	Max. 3.2 dB
Çıkış VSWR	Max. 2.0	Max. 2.0
Toplam Kazanç	Typ. 21.4 dB	Typ. 21.4 - 22.4 dB

Ek olarak antenin radyasyon desenleri Şekil 5-9 ve Şekil 5-10'da gösterilmiştir.



Şekil 5-9 Radyasyon Desenleri L1 Bandı. 2-D kesikler 1559 - 1606 MHz aralığında ölçülmüştür.



Şekil 5-10 Radyasyon Desenleri L2 Bandı. 2-D kesikler 1197 - 1249 MHz aralığında ölçülmüştür.

5.1.6.2. GGB236 anteni

GGB236 anteni, Ann-Mb-00-00 anteni gibi yüksek hassasiyetli aktif GNSS anteni olarak geçer [45]. İçindeki anten ve düşük gürültülü güç yükseltecinin özellikleri sırasıyla Çizelge 5.10 ve Çizelge 5.11'de verilmiştir.

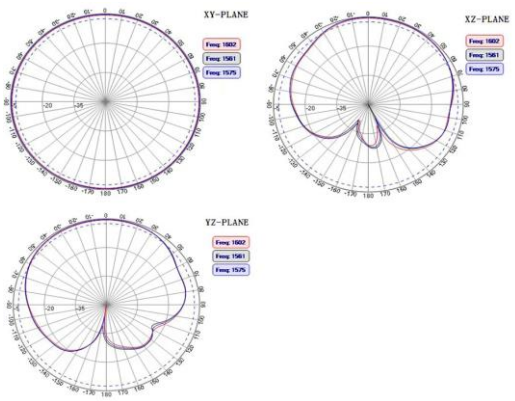
Çizelge 5.10 - Anten parametreleri

Parametre	L1 Bandı
Frekans	1561.098 - 1602 MHz
Empedans	50 Ω
Kazanç	5 dBic (Zenith)
Polarizasyon	RHCP
Axial oran	Max. 3.0 dB (Zenith)

Çizelge 5.11 - Düşük gürültülü güç yükselteci paramatreleri

Parametre	L1 Bandı
Frekans	1561.098 - 1602 MHz
Empedans	50 Ω
LNA Kazancı	Typ. 28 ± 2.0 dB
Gürültü Şekli	Max. 1.5 dB
Çıkış VSWR	Max. 2.0

Ek olarak antenin radyasyon desenleri Şekil 5-11'de gösterilmiştir.



Şekil 5-11 Antenin Radyasyon Deseni

5.1.6.3. CRPA anteni

Yukarıda anten tabanlı aldatma yöntemlerinde de bahsedildiği üzere CRPA antenler karıştırma ve aldatma saldırılarına karşı kullanılan çok etkili bir yöntemdir. Yönlü desen oluşturmak için birden fazla anten elemanı kullanarak havadaki uydudan gelen sinyaller ile aldatma saldırısı için üretilip farklı açılardan yayınlanan sinyalleri birbirinden ayırt edebilir. Bu antenler ileri teknolojisi ve içerisinde ek olarak bulunan sinyal işleme kapasitesi nedeniyle kompleks ve pahalı cihazlardır. Bu çalışmada da TUALCOM şirketinin tasarlayıp ürettiği Şekil 5-12'te görülen TUALAJ-4300-D anteni kullanılmıştır. Bu antenin içinde 4 adet faz dizili anten bulunmaktadır ve bu 4 elemanlı CRPA anteni sayısal kontrolcü ve çeşitli hüzme oluşturma teknikleri ile 3 farklı frekans bandında 3'e kadar sinyal karıştırma kaynağına karşı karıştırma sinyallerini bastırabilir. Bu antenin teknik özellikleri Çizelge 5.12'de verilmiştir [45].

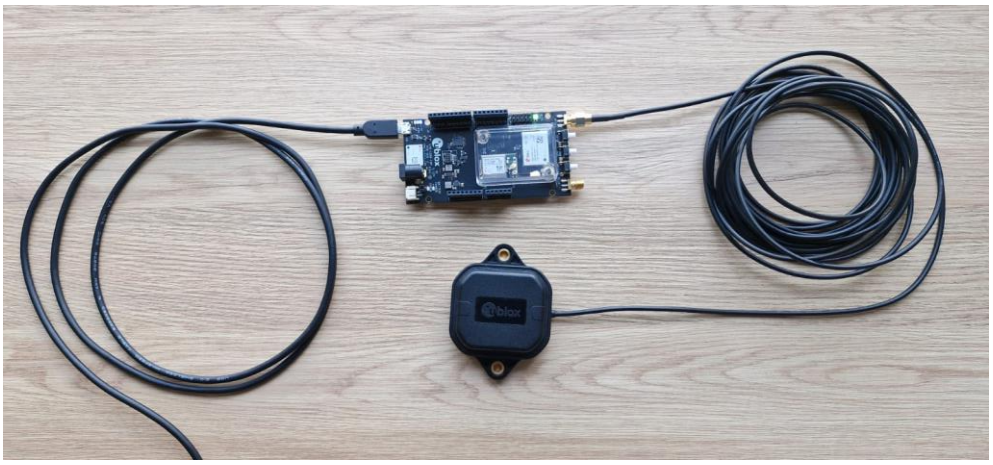
Çizelge 5.12 - CRPA anteni teknik özellikleri

Parametre	Özellikleri
Güç Tüketimi	18W max.
Çalışma Voltajı	12-28 Vdc
Çalışma Sıcaklığı	-40 °C to +85 °C
Anten Dizisi	4 Dizi CRPA anteni
Simülatene Olarak Koruduğu Aktif Bantlar	GPS (L1, L2), GLONASS (G1, G2), GALILEO E1, BEIDOU B1, SBAS
Nominal Genişbant Bastırması	>40 dB
Çevre Koşulları Testi	MIL-STD-810G
EMI/EMC Testleri	MIL-STD-461F

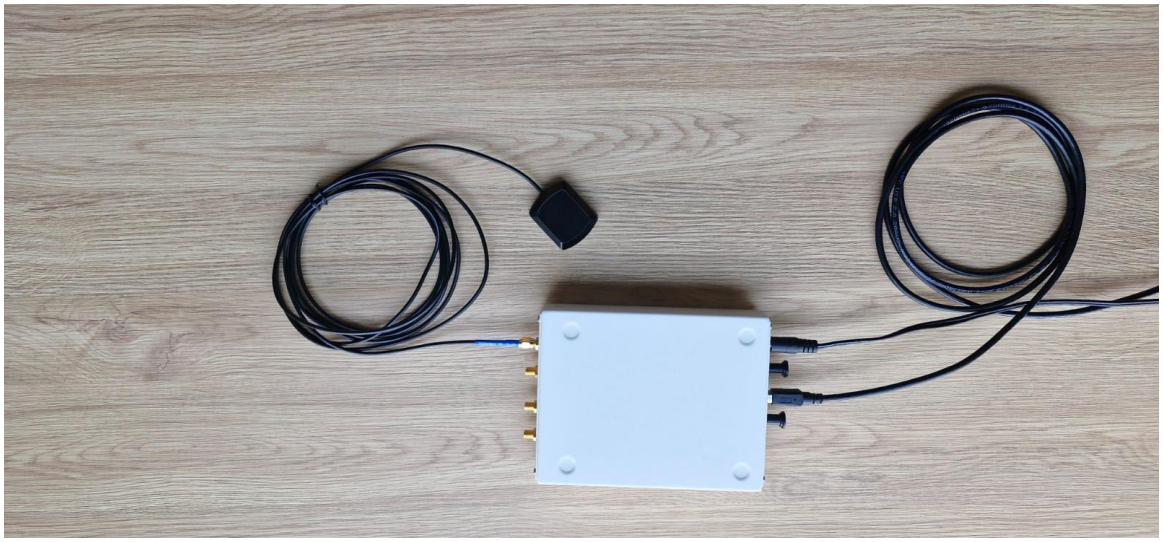
Şekil 5-12 TUALAJ-4300-D CRPA Anteni

5.2. Aldatıcı Kurulum Çalışmaları

İlk olarak u-blox C099-F9P uygulama kartı (GNSS alıcısı) ve u-center arayüzü kullanılarak kapalı alanda çeşitli çalışmalar yapılmıştır. Bu çalışmalarda NI USRP-2901 cihazı ve Labview programı kullanılarak oluşturulan GPS simülatöründen GPS sinyali üretilerek GNSS alıcısını kandırmaya yönelik çalışmalar yapılmıştır. Bu çalışmalarda kapalı alanda GNSS alıcısı açılıp GPS simülatöründen uydu sinyali üretilip basılmıştır. GNSS alıcısının çıkışına Şekil 5-13'te görüldüğü gibi ANN-MB-00-00 anteni; GPS simülatörünün çıkışına Şekil 5-14'te görüldüğü gibi GGB236 anteni bağlanmıştır.

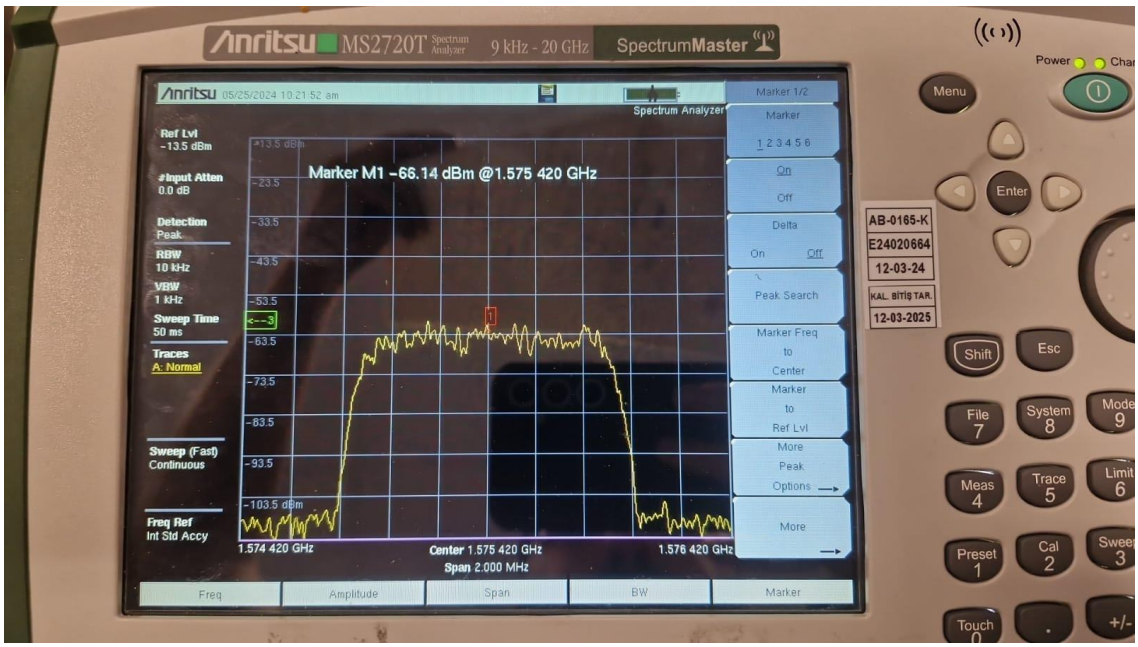


Şekil 5-13 GNSS Alıcısına Bağlanan u-blox Anteni



Şekil 5-14 USRP Cihazına Bağlanan GGB236 Anteni

GPS simülatöründen GPS sinyal yayılımı yapıldıktan sonra USRP cihazının anten çıkışından spektrum analizör ile ölçüm alındığında analizör ekranında Şekil 5-15'te görüldüğü gibi bir görüntü elde edilmiştir.



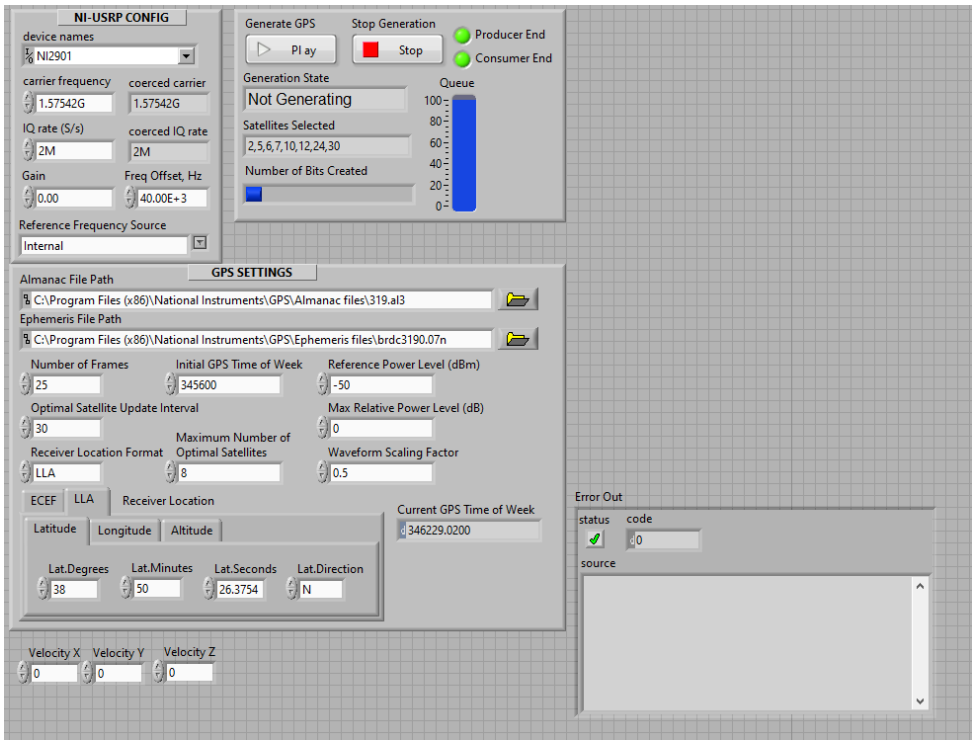
Şekil 5-15 USRP Anten Çıkışı

GPS simülatörünün ayarları ise Şekil 5-16'da verilmiştir. Bu konfigürasyonda 0 dB kazanç vererek toplamda 25 adet bölümden oluşan yaklaşık (12.5 dk. ya denk

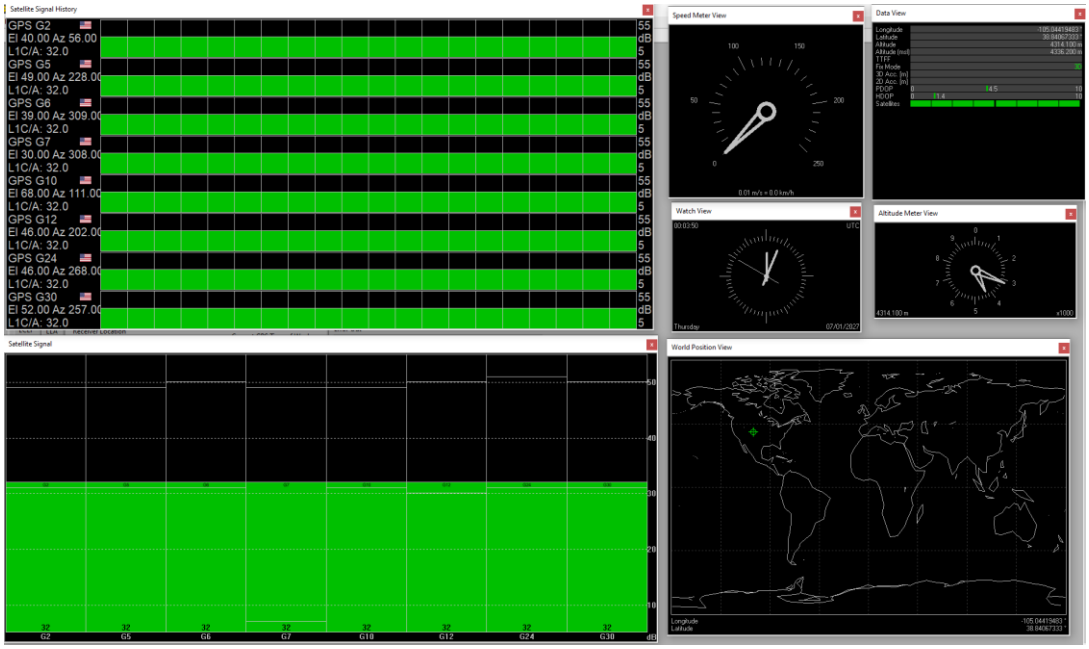
gelmektedir) 2027 yılına ait hızı olmayan ve enlem, boylam ve yükseklikleri de sırasıyla 38,84066; 105.044087; 4302 olan konfigürasyon girilmiştir.

GNSS alıcısı uydudan herhangi bir sinyal alamadığı için ilk açıldığında doğrudan olarak GPS simülatöründen yayınlanan sinyali almakta ve o sinyale kilitlenmektedir. Alıcının GPS simülatörüne kilitlendiğini u-center programından Şekil 5-17 ve Şekil 5-18'de gösterilen görseller incelenerek anlaşılabilir.

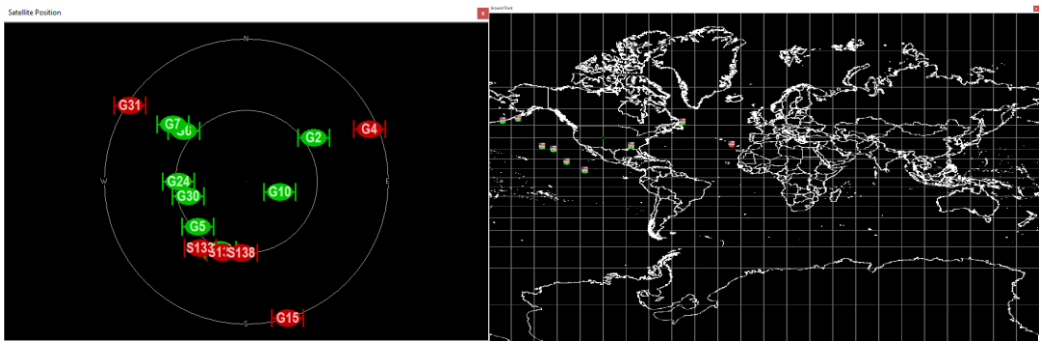
Ek olarak GNSS alıcısı bu sinyale kilitlendikten sonra açık havaya çıkartıldığında gerçek olan sinyali bir aldatıcı sinyal olarak algılayıp ilk kilitlendiği sinyali almaya çalışmaktadır. Eğer alıcının ilk aldığı sinyal de kesilirse cihazın gösterdiği konum verisi kesiliyor ve yaklaşık 10 dk. kadar sadece saat verisi geldikten sonra saat verisi de kesilip açık havadaki sinyale kilitleniyor. Buradan da anlaşılacağı üzere GNSS alıcısında bulunan algoritmada da bir aldatma karşıtı tedbir olan, konumda ani atlamalara karşı bir yöntem bulunmaktadır. Fakat uzun süreli aldatma ve karıştırmalarda aldatıcıya yenik düşmektedir.



Şekil 5-16 GPS Simülatörü Konfigürasyonu



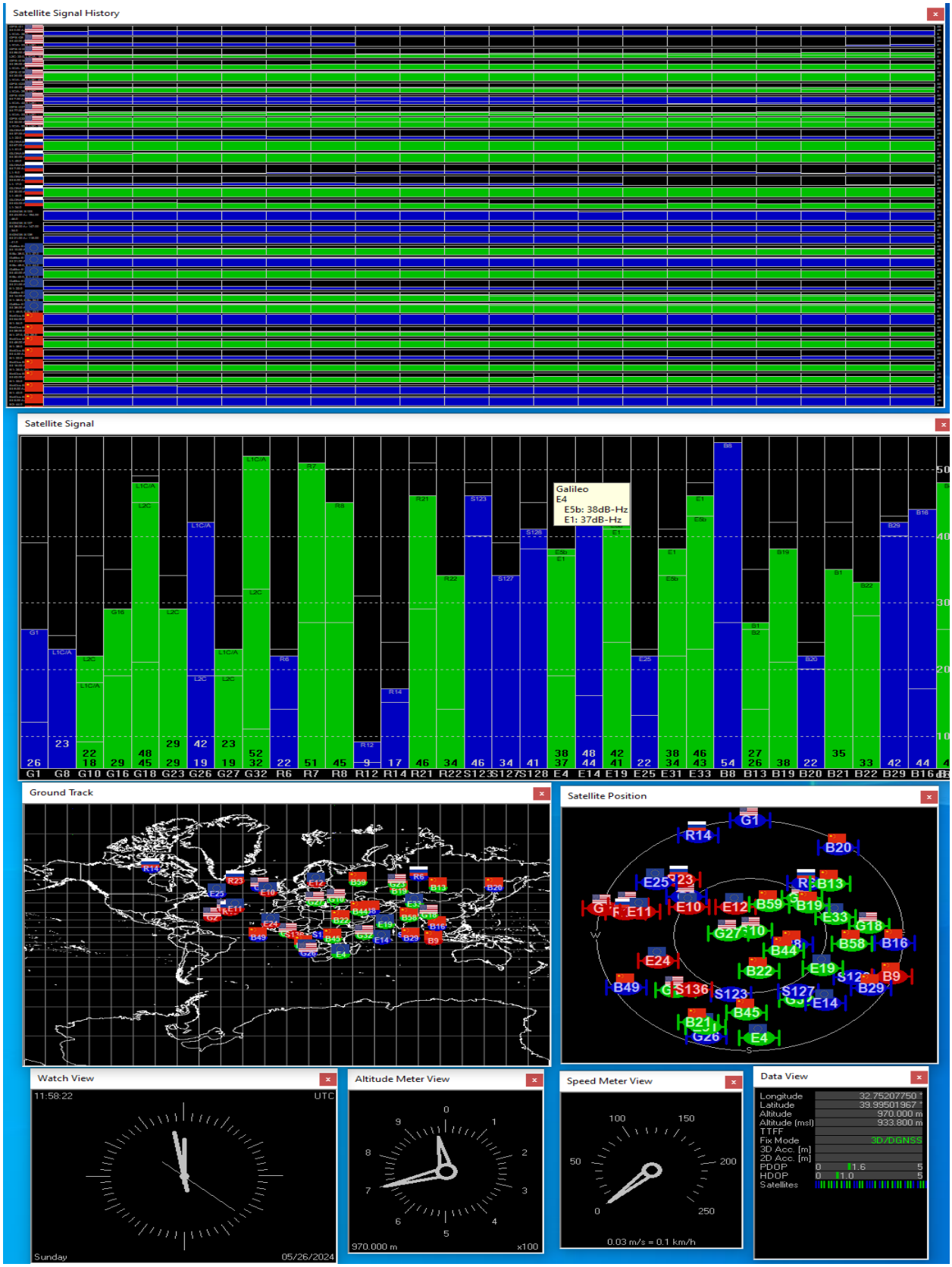
Şekil 5-17 GNSS Alıcısı Konum Çözümü u-center Arayüzü



Şekil 5-18 GNSS Alıcısı Uydu Çözümü u-Center Arayüzü

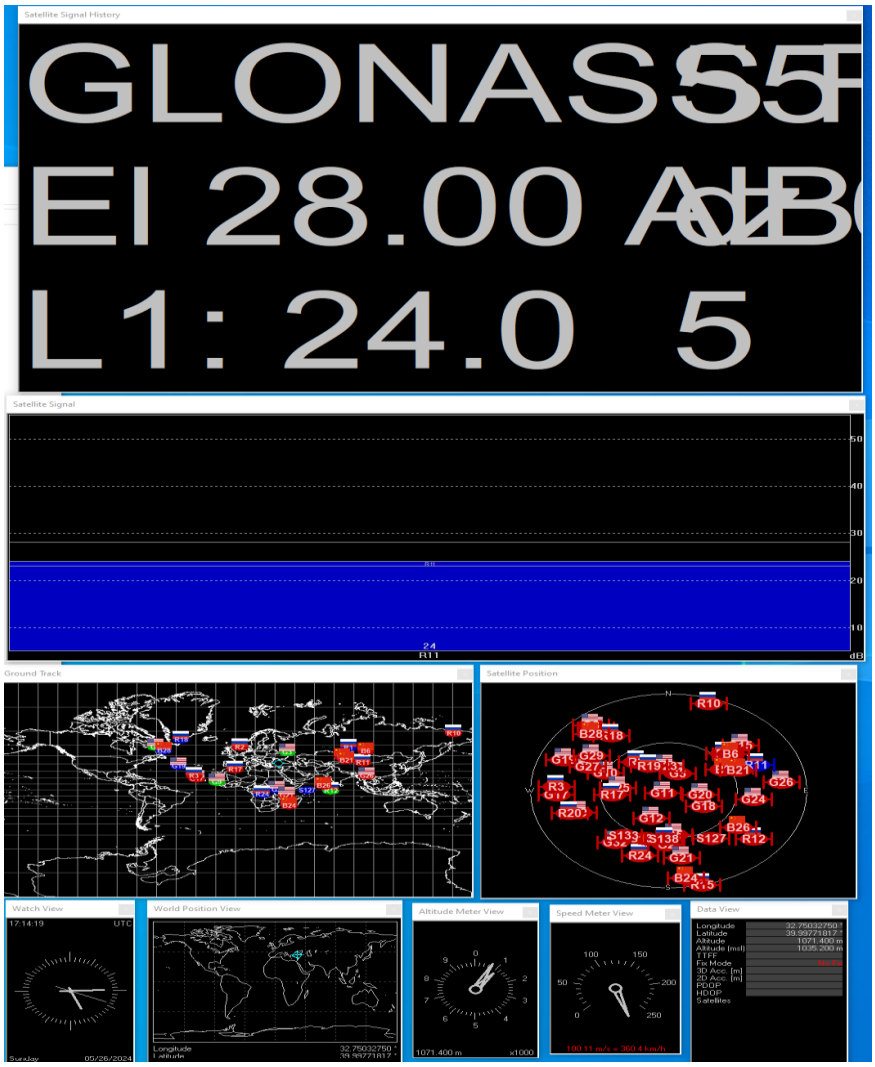
Ardından GNSS alıcısını ilk önce açık havada bulunan sinyalleri alması, ardından alıcı açık havada iken aldatma sinyali yayılımı yapılıp GNSS alıcısına aldatma saldırısı gerçekleştirilmeye çalışılmıştır. Bu saldırıda yine güncel almanac ve efemeris kullanmak yerine 2027 tarihinde olan veri seti kullanılmıştır. İlgili kurulum Şekil 5-19‘ da gözlemlenebilir. GNSS alıcısının anteni açık alana konulduktan sonra GNSS alıcısı uydu sinyallerini almaya başlamıştır. Alınan sinyaller Şekil 5-20‘ de gözlemlenebilir. Farklı konstelasyonlardan sinyalleri yakalayabilen alıcı, konum çözümünü uygun bir şekilde çıktı olarak çıkartmaktadır. Bu kurulumun ardından GPS simülatöründen L1 bandında yüksek güçlü bir GPS sinyali yayılmıştır fakat bu denemelerde uzun süre beklense de GNSS alıcısı aldatılamamıştır.

Şekil 5-19 Aldatıcı Test Düzeneği Yerleşimi



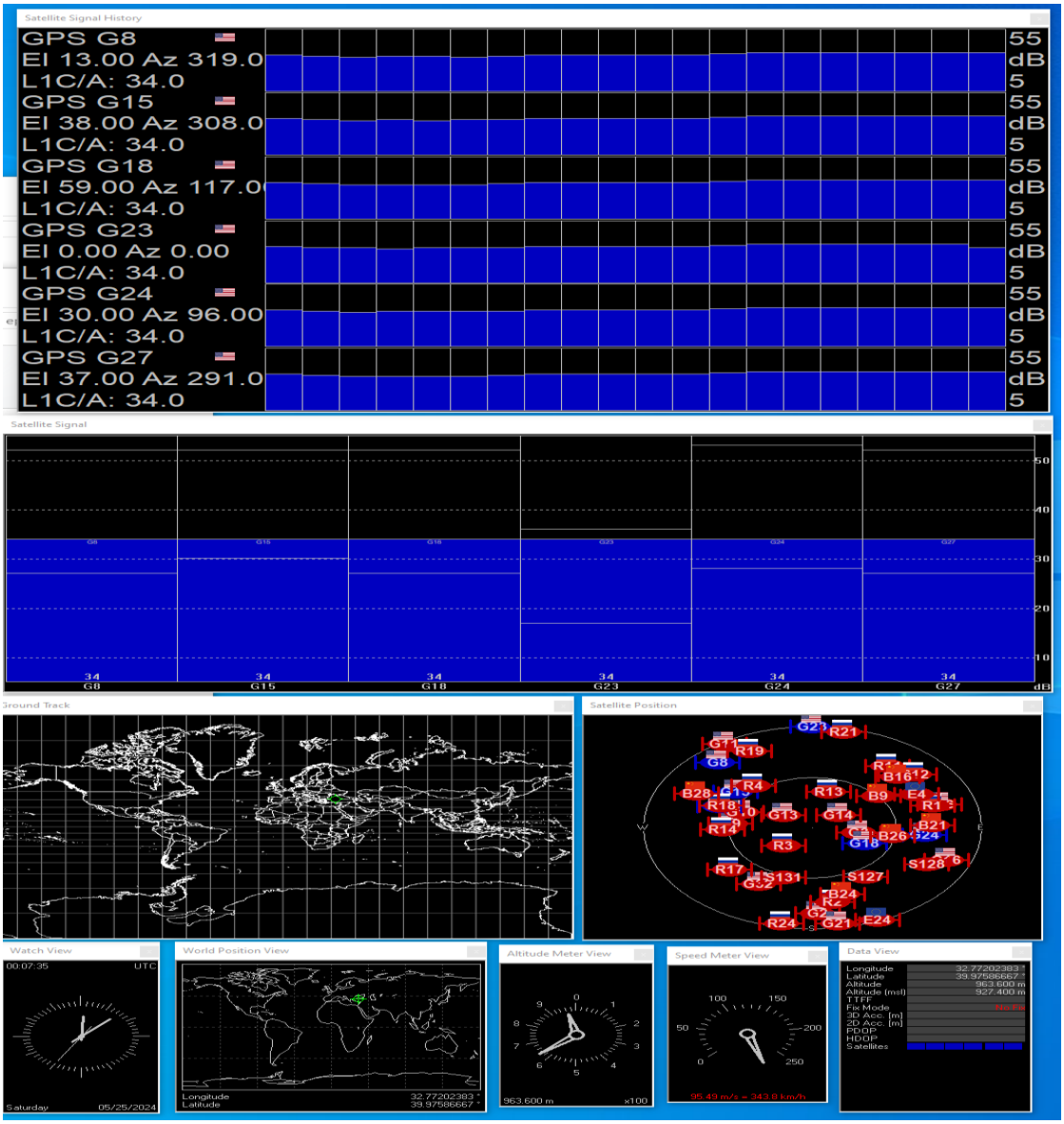
Şekil 5-20 GNSS Alıcısının Açık Alanda Alabildiği Uydu Sinyalleri

Alıcı GPS L1 bandından sinyal alamasa da diğer uydulardan gelen sinyallere kilitlendiği için ve bu uydulardan gelen sinyallere karşı kilidi kırılmadığı için aldatma saldırısı başarıya ulaşamamıştır. Fakat ardından bu alıcıyı aldatmak için diğer frekans bantlarına da karıştırma sinyali uygulama yöntemi denenmiştir. Bu yöntemde ise Anritsu 3692c sinyal üretecinin RF çıkışına bir anten bağlanıp 1602 MHz merkezli 0 dBm büyüklüğünde bir sinyal yayılımı yapması sağlanmıştır. Bu şekilde zaten GPS simülatörü kullanılarak yüksek güçte basılan yayılan ile gerçek GPS sinyali ve Galileo sinyalleri bastırılacak ve sinyal üreteci ile de GLONASS sinyalleri yayılımı yapılıp GNSS alıcısı aldatılmaya çalışılacaktır. Bu yöntemde GPS simülatörü ve sinyal üreteci çalıştırıldığında ilk karşılaşılan ekran Şekil 5-21'de gösterilmiştir.



Şekil 5-21 Aldatma Saldırısı Başladığında GNSS Alıcısının Konum Çözümü

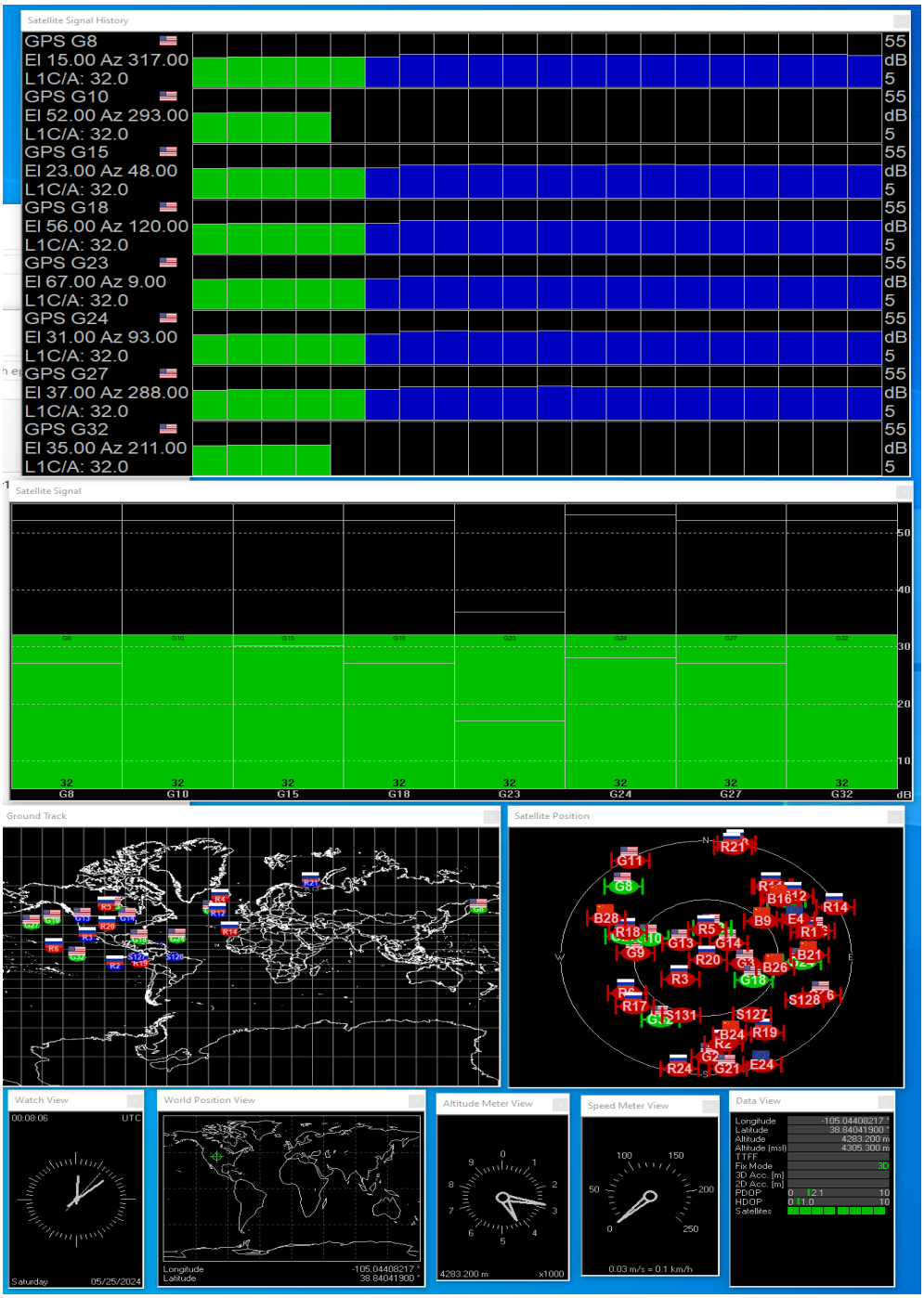
İlgili şekil detaylı şekilde incelendiğinde konumda herhangi bir değişiklik olmamasına rağmen konum çözümündeki 3D fix in No fix'e dönüştüğü, hızın aniden 360.4 km/h olarak ölçüldüğü ve konum çözümlerinin de farklı bir şekilde değiştiği gözlemlenmiştir. Aldatma saldırısından birkaç dakika geçtikten sonra sinyal üretecinden karıştırma sinyali kaldırılmış ve Şekil 5-22 gözlenmiştir.



Şekil 5-22 Karıştırma Saldırısı Sonlandırıldıktan Sonra GNSS Alıcısı Konum Çözümü

İlgili şekilde de görüldüğü gibi karıştırma saldırısı sonlandırıldıktan sonra GNSS alıcısı GPS simülatörü tarafından uydu sinyalinden daha yüksek güçte yayınlanan

L1 sinyallerine kitlenmiştir. Alıcı, GPS simülatörü tarafından yayınlanan tarih ve saati çözüyor fakat hala konumu eski aldığı konum olarak gösteriyor ve hızı da hala 343.8 km/h gibi farklı bir sayı belirtiyor. Bu da hala aldatma saldırısının altında olduğuna işaret ediyor. Aradan birkaç dakika geçtikten sonra Şekil 5-23 gözlemlenmiştir.



Şekil 5-23 GNSS Alıcısının Aldatma Sinyaline Kilitlenmesi

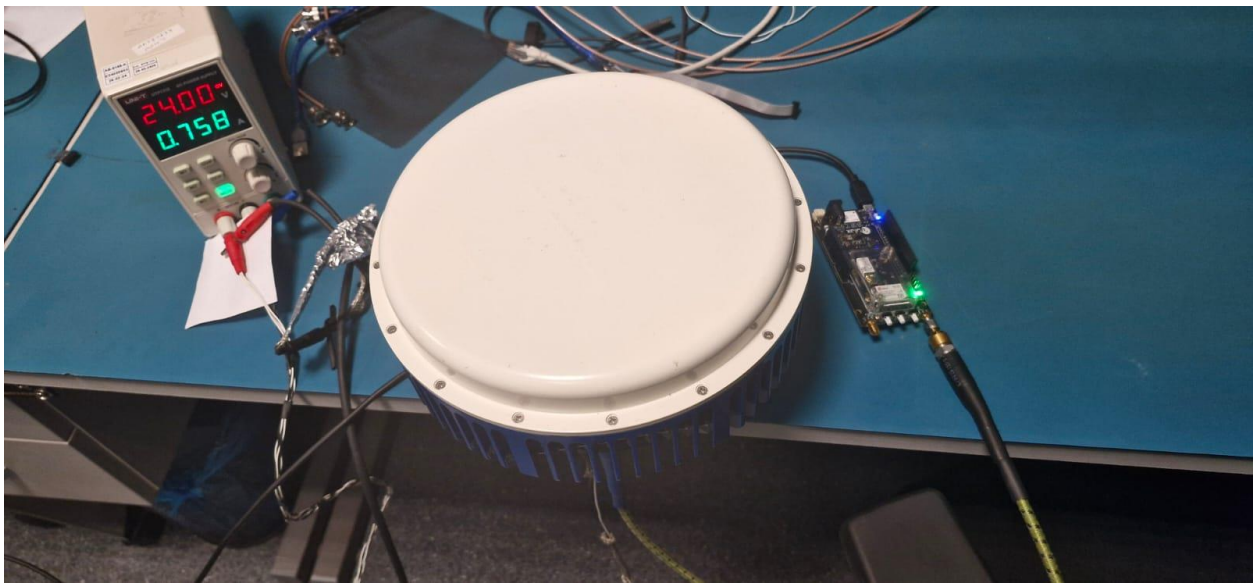
İlgili şekilde de görüldüğü gibi aldatma saldırısı başarılı olmuş; GNSS alıcısı GPS simülatörü tarafından yayılan aldatma sinyaline kilitlenmiş ve konum çözümünü de doğrulamış olarak GPS simülatörü tarafından belirlenmiş ABD'de bulunan bir konumu göstermektedir. Buradan da anlaşılacağı üzere GNSS alıcılarının çalıştığı bantlarda karıştırma sinyali uygulandığında GNSS alıcılar da aldatılabilir.

5.3. Aldatma Karşıtı Önlemler

Yapılan deneysel çalışmalar CRPA anten ile yapılan çalışmalar ve IMU sensörü ile yapılan çalışmalar olarak 2 ana başlıkta incelenmiştir.

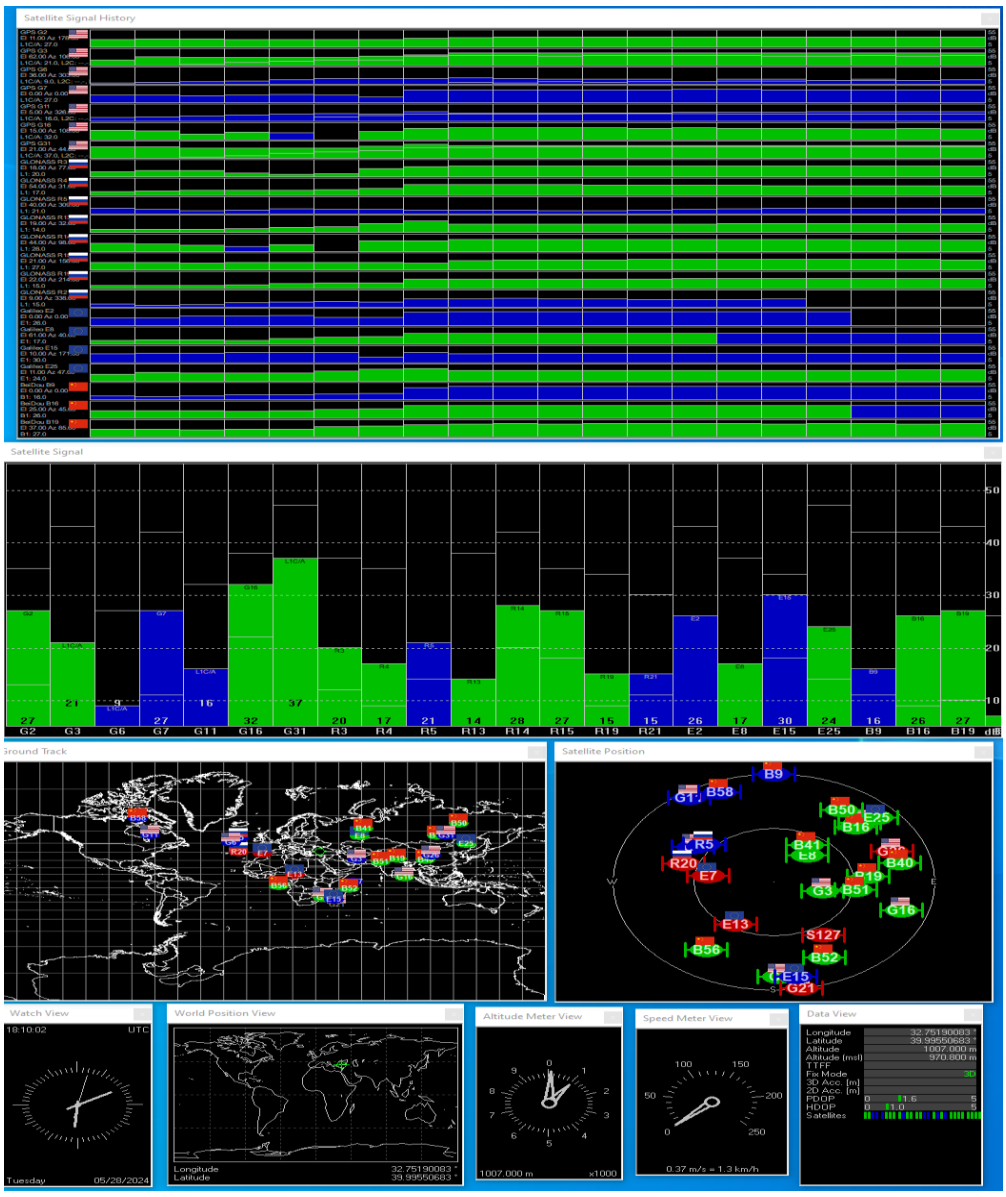
5.3.1. CRPA Anten ile Yapılan Çalışmalar

Bu çalışmada ilk olarak GNSS alıcısına CRPA anten takılarak, USRP cihazından uydu sinyali yayını yapılıp CRPA anteninin aldatma saldırılarına karşı ne kadar dayanıklı olduğu, Şekil 5-24'te gösterilen kurulum ile test edilmiştir. İlk olarak kapalı alanda testler yapılmış olup kapalı alanda yapılan testlerde CRPA anteni herhangi bir uydu sinyali alamadığında ve sadece yüksek seviyede USRP cihazından yayınlanan GPS sinyalini aldığındaki tepkisi test edilmiştir. Bu çalışmada GNSS alıcısı ilk açıldığında doğrudan sahte uydu sinyalini aldığı ve başka uydu sinyali alamadığı için GPS simülatörü tarafından yayınlanan saat ve konumu gerçek konum gibi algılamıştır.



Şekil 5-24 GNSS Alıcısı İle Kullanılan CRPA Anteni

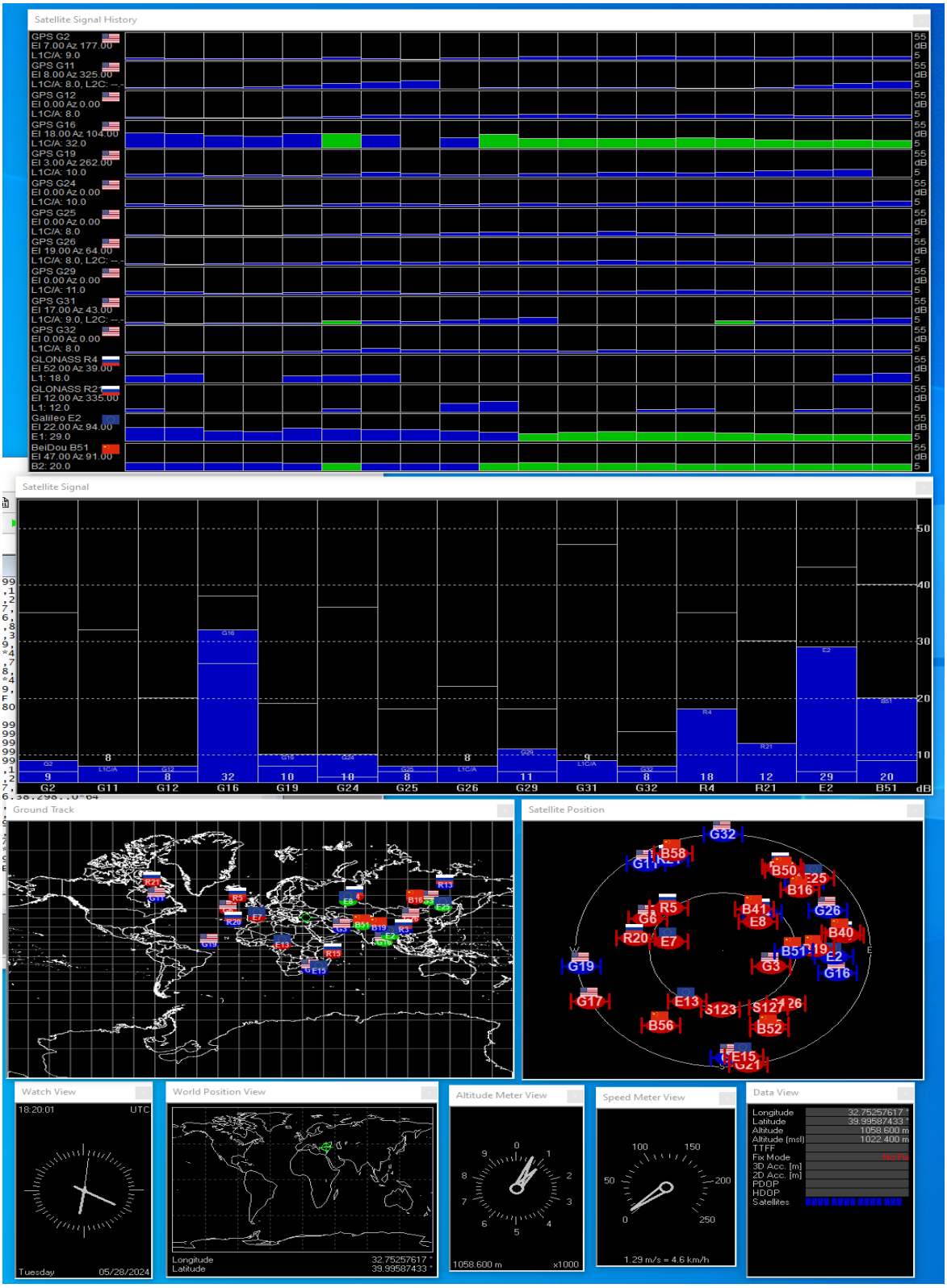
Ardından yapılan çalışmada CRPA anteni ilk olarak açık havada bırakılmış ve bir süre açık havada gerçek uydu sinyallerine kilitlenmesi beklenmiş ve ardından GPS simülatöründen yüksek seviyede sahte uydu sinyali basılıp sinyal üreteçlerinden karıştırma sinyalleri yayınlanmıştır. Bu şekilde GPS L1, GLONASS G1, Galileo E1 ve BEIDEU B1 sinyallerinin antene ulaşması engellenecektir. Ardından karıştırma sinyalleri kapatılıp CRPA anteninin GPS simülatörü tarafından gönderilen sahte GPS sinyaline kilitlenmesi sağlanacak ve aldatma saldırısı başarıyla gerçekleşecektir.



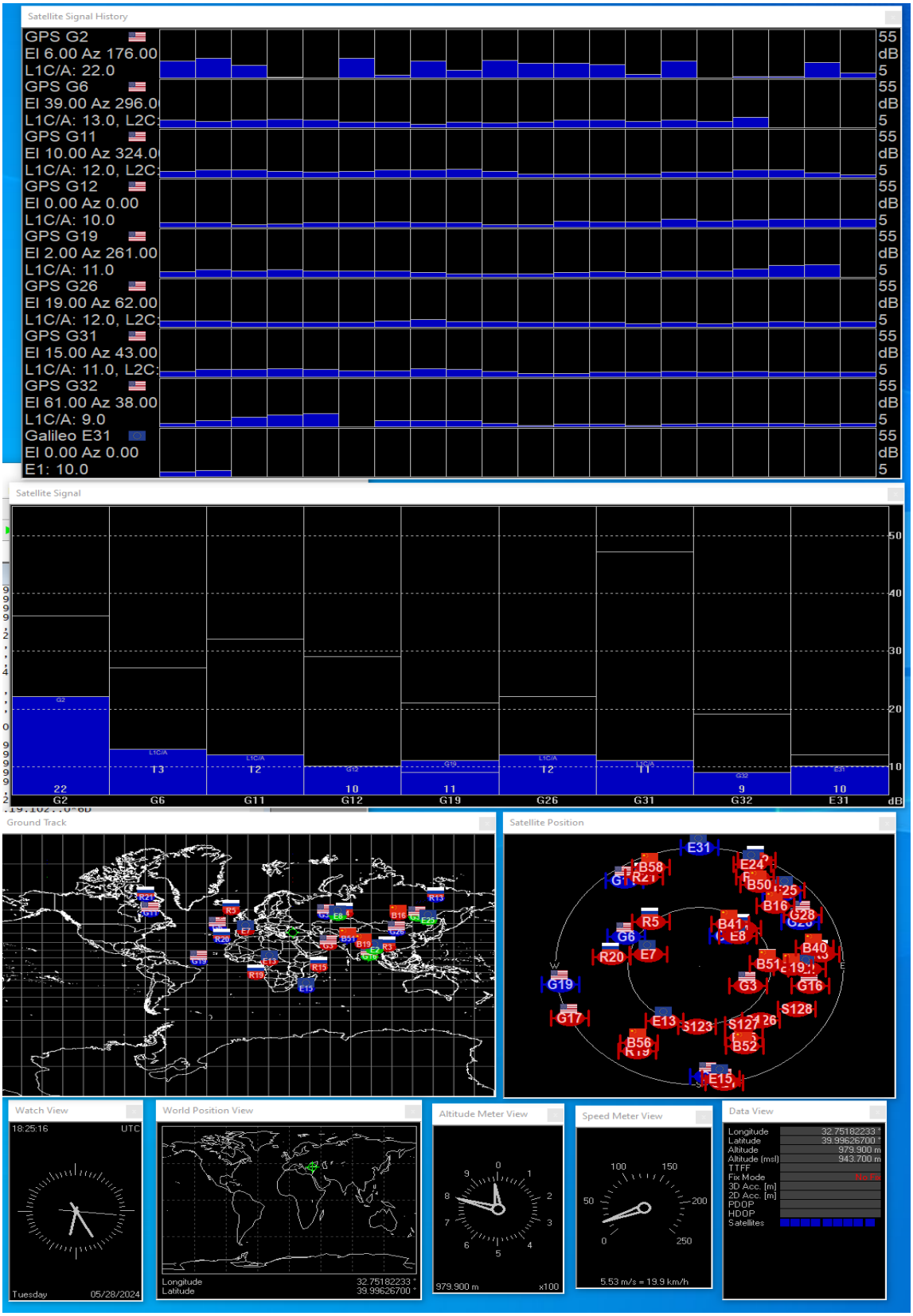
Şekil 5-25 CRPA Anten Açık Havadayken GNSS Alıcısı Tarafından Çözümlenen Sinyaller

İlk aşamada CRPA anteni açık havaya çıkratıldığında GNSS alıcısının kilitlendiği sinyaller Şekil 5-25'te gösterilmişti. Görselden de görüleceği üzere GPS L1, Galileo E1, GLONASS G1, Beideu B1 sinyalleri alınmaktadır. Ayrıca konum, hız ve saat çözümlerinde de herhangi bir tutarsızlık bulunmamaktadır. Bu konumdayken sinyal üreteçlerinden 10dBm 1602 MHz frekansında; 7dBm 1561.098 MHz bandında karıştırma sinyalleri yayınlanmış olup, GPS simülatörü cihazından L1 bandında sinyal yayını yapılmaya başlanmıştır. Fakat burada belirtmek gerekir ki anten konumları bu kısımda önem arz etmektedir. CRPA antenler yan ve aşağıdan gelen sinyalleri bastırdıklarından dolayı ve uydu sinyalleri de yukarıdan geldiğinden dolayı bu karıştırma sinyalleri uydudan gelen sinyalleri bastırmada yeterli olmayabilir. Karıştırma sinyallerinin ve aldatma sinyalinin yayıldığı antenler uygun konuma getirildikten sonra karıştırma ve aldatma sinyalleri uygulanmıştır. Ardından bir süre beklenilmiş (yaklaşık 10 dk.) olup bu süre boyunca GNSS alıcısının önceden kilitlendiği sinyallerin seviyelerinin düşmesine rağmen konum 3D-fix şeklinde kalmıştır. Bu süre sonunda konum 3D-fix ten no-fix şekline geçmiştir fakat Şekil 5-26'da görüldüğü gibi hala saat ve konum doğrudur. Bu kurulum sabit bir yerde yapıldığından dolayı GNSS alıcısının alabildiği en son konum kalmış ve biz bir hızda hareket etsek bile bu hareketi algılamayıp en son aldığı konumu gösteriyor olacaktır. Bu çalışmada bu kurulum haraketli bir platformda yapılmamıştır.

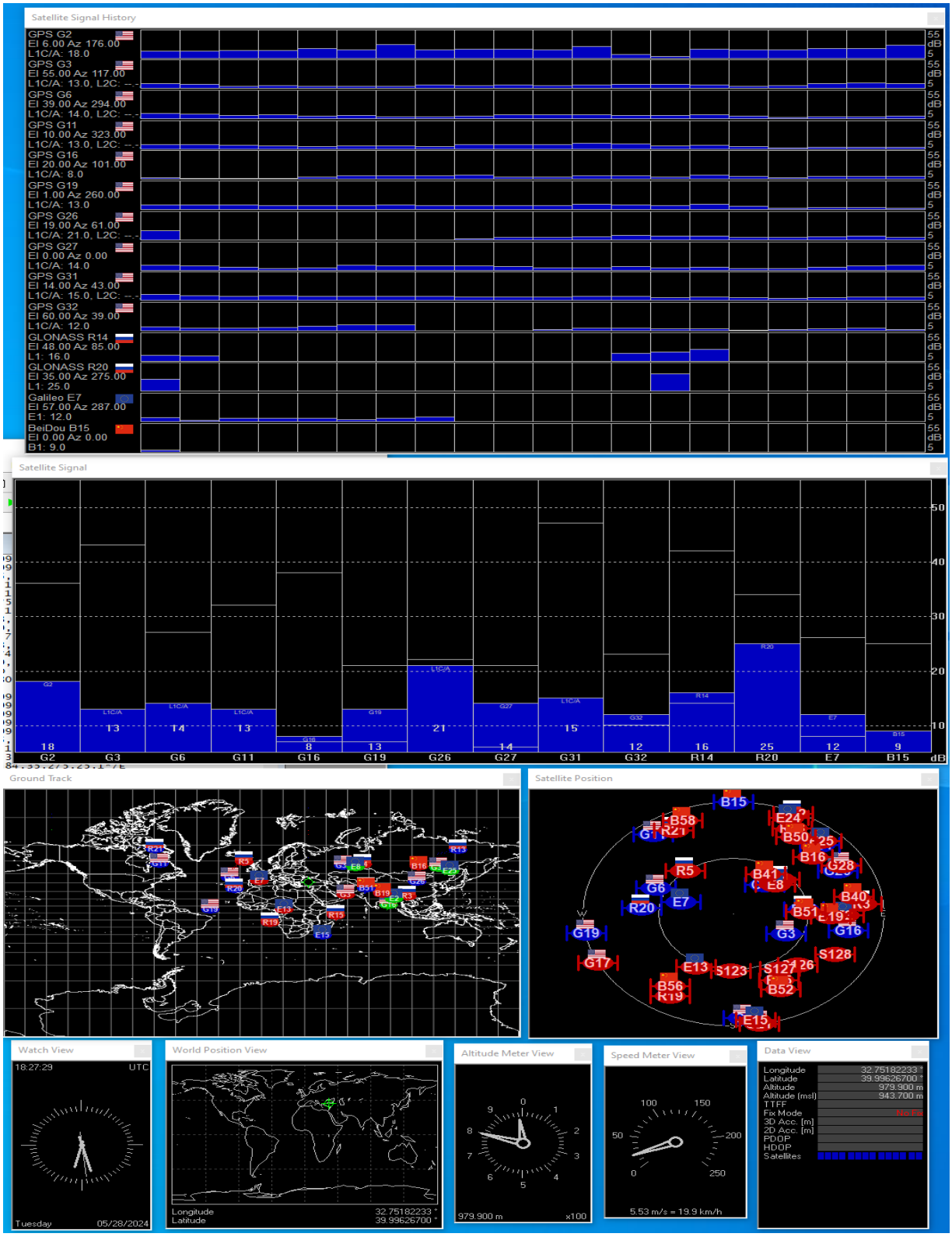
Bir süre daha (yaklaşık 5 dk.) geçtikten sonra karıştırma sinyalleri kesilmiştir ve sadece GPS simülatöründen basılan GPS sinyali yayını kalmıştır. Şekil 5-27'de görüldüğü gibi GNSS alıcısı sadece GPS simülatöründen yayınlanan sinyalleri alıyor ve diğer sinyalleri alamamaktadır. Geçen süre içerisinde farklı uydulardan düşük seviyede sinyal alabilse de bu sinyal seviyeleri düşük olduğu için Şekil 5-28'de görüldüğü gibi bu sinyallere kilitlenememekte ve konum çözümünü yapamamaktadır.



Şekil 5-26 Karıştırma ve Aldatma Saldırısının Üzerinden Bir Süre Geçtikten Sonra GNSS Alıcısı Konum Çözümü

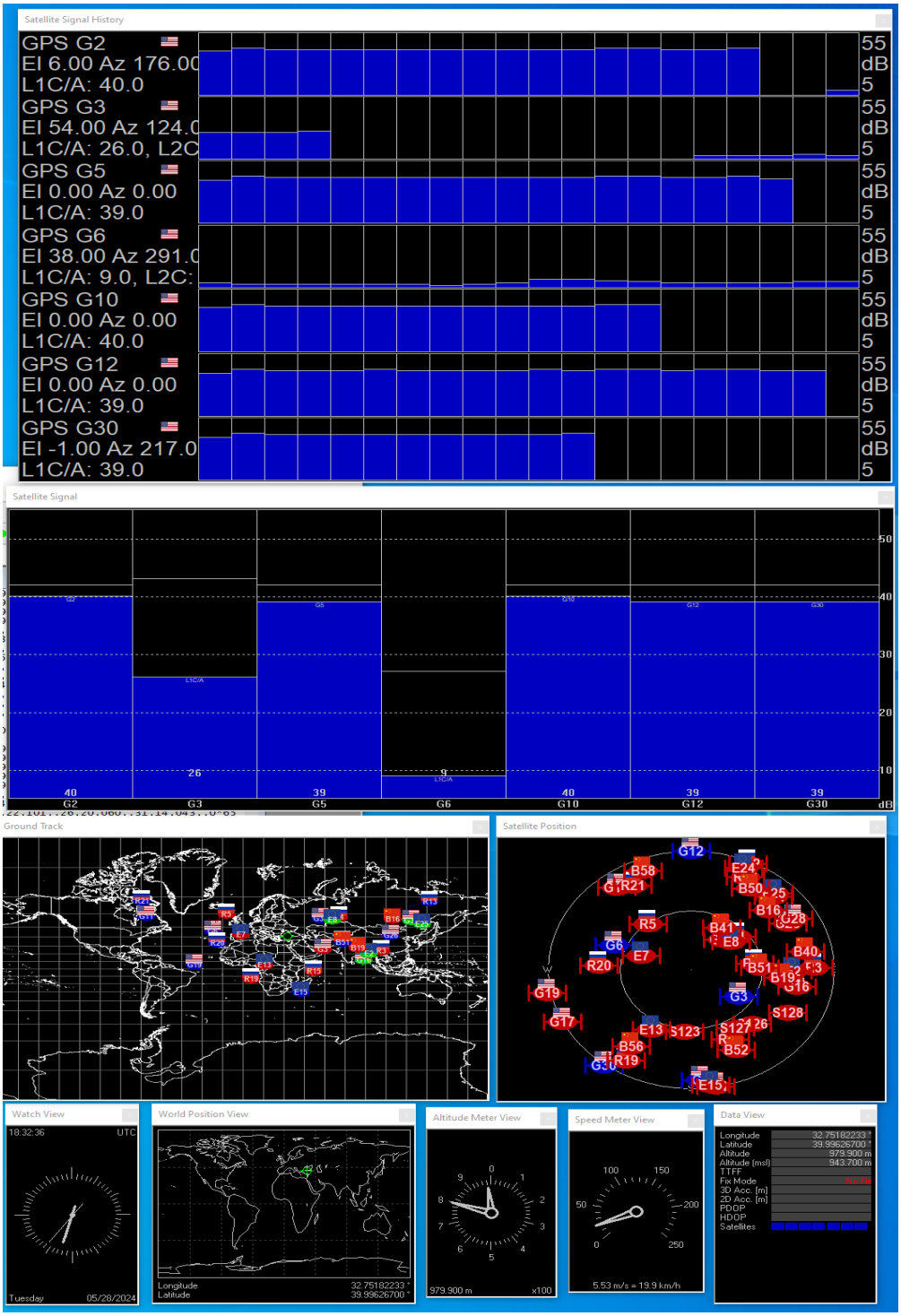


Şekil 5-27 Karıştırma Sinyalleri Kesildikten Sonra GNSS Alıcısının Aldığı Sinyallerin Gösterimi



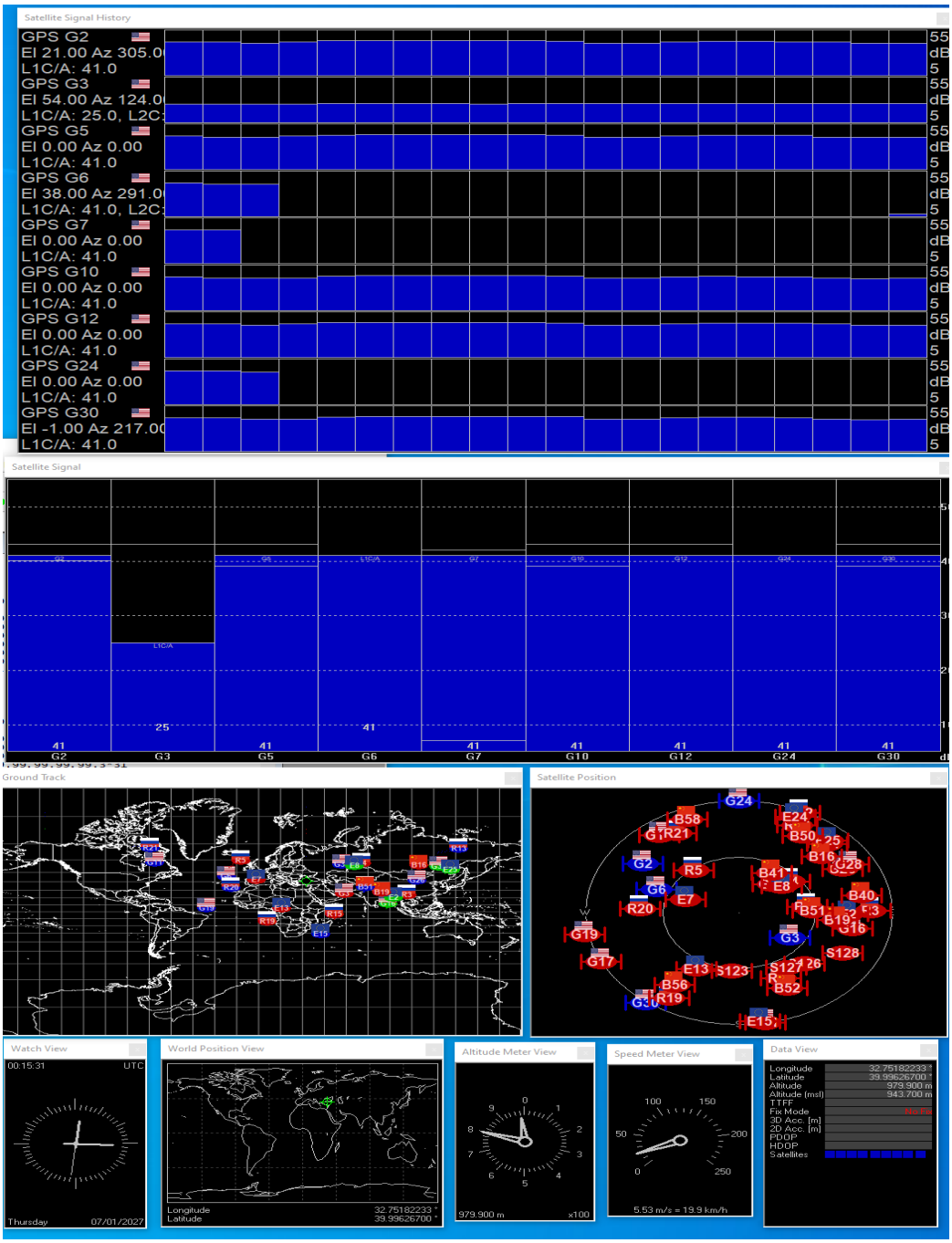
Şekil 5-28 Karıştırma Sinyalleri Kesildikten Sonra GNSS Alıcısının Düşük Seviyede Aldığı Uydu Sinyalleri

Aradan bir süre geçtikten sonra Şekil 5-29'da görüldüğü gibi GNSS alıcısı saati kaybetmiş ve GPS simülatörü tarafından yayınlanan tarihi ve saati çözmeye başlamıştır.



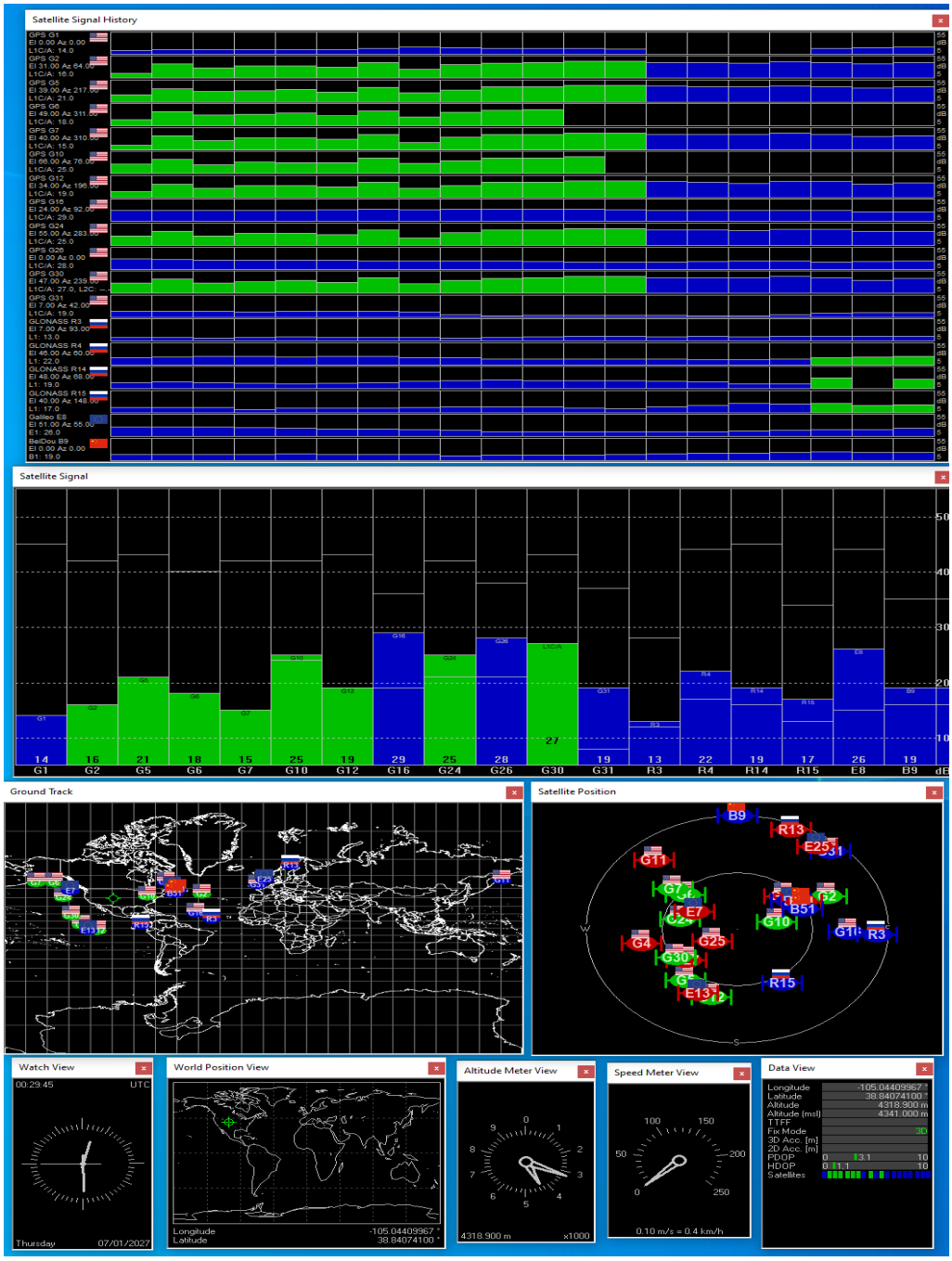
Şekil 5-29 GNSS Alıcısının Saati ve Tarihinin Değişmesi

Yeteri kadar vakit geçmesine ve GNSS alıcısı sadece GPS simülatöründen yüksek seviyede yayılan sinyali almasına rağmen, ayrıca saati de GPS simülatöründen gelen sinyallerle çözerken GNSS alıcısı Şekil 5-30'da görüldüğü gibi doğrulanmış konum çözümü vermemekteydi.



Şekil 5-30 Süre Geçmesine Rağmen GNSS Alıcısının GPS Simülatöründen Yayılan Sinyalleri Alarak Konumu Çözmemesi

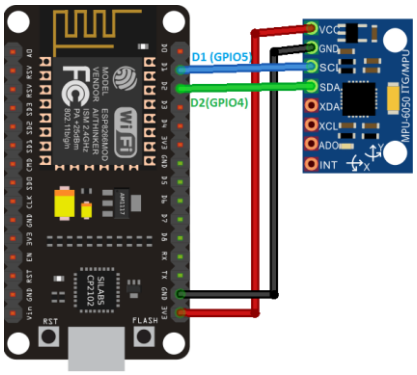
Ardından CRPA anten özelliği olarak yüksek seviyede gelen sinyali, aldatma sinyali olarak algıladığı anlaşıldı ve GPS simülatöründen sinyal seviyesi düşürüldü. Sinyal seviyesi belli bir eşiğin altına geldiğinde GNSS alıcısı Şekil 5-31'de görüldüğü gibi GPS simülatöründen yayılan sinyali çözmeye ve gerçek konum olarak GPS simülatöründe ayarlanan konumu göstermeye başlamıştır.



Şekil 5-31 GNSS Alıcısının Aldatma Sinyallerini Alıp Sahte Konumu Göstermesi

5.3.2. IMU Sensörü ile Yapılan Çalışmalar

Aldatma karşıtı almaç mimarisinde bahsedilen denklemler, bir IMU sensör ve sivil GNSS alcısı ile gerçeklenmek istenmiş ve bu başlık altında da buna yönelik çalışmalar anlatılmıştır. IMU sensörü ivmeölçer olarak kullanıp bu sensörden alınan x, y ve z eksenindeki ivmelenme verileri işlenmiş ve ivmelenmenin büyüklüğü ve hızın büyüklüğü bulunmuştur. Bu işlemler yapılırken MPU9250 sensörü kullanılmıştır. Fakat MPU9250 sönsörü yerine ADXL345 gibi üç eksenli ivmeölçer sensörler de kullanılabilir. İşlemci olarak ESP8266 NodeMCU Şekil 5-32'de gösterilen bağlantılar ile Arduino IDE kullanılarak kodlanmıştır. Burada da ESP8266 NodeMCU yerine Arduino gibi işlemciler kullanılabilir.



Şekil 5-32 İşlemci İle Sensör Arasındaki Bağlantı

İvmeölçer sensöründen alınıp işlenmesi için yazılan Arduino kodu aşağıdaki Şekil 5-33'te gösterilmiştir.

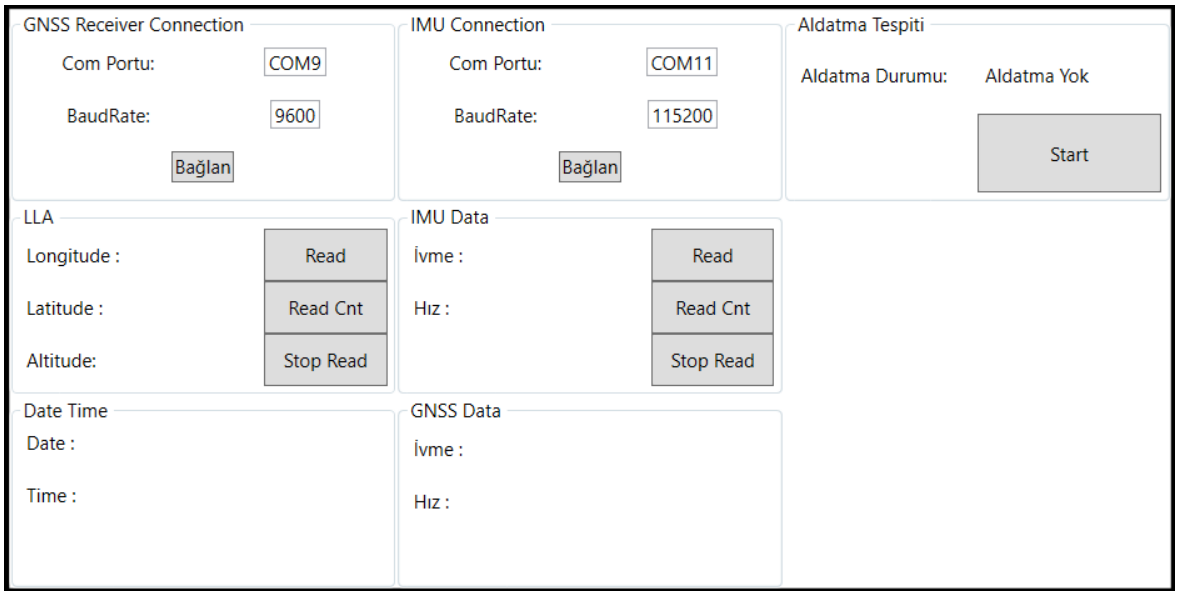
```ino
#include <Wire.h>
#include <MPU9250.h>

#define SDA_PIN D2
#define SCL_PIN D1

MPU9250 mpu;

float ax, ay, az; // Acceleration values
float vx = 0, vy = 0, vz = 0; // Velocity values
unsigned long previousTime = 0;
float magVel, magAcc;

float accBias[3] = {0.28, 0.02, -0.05};
float gyroBias[3] = {-1.28, 1.04, -0.52};


void setup() {
  Serial.begin(115200);
  Wire.begin(SDA_PIN, SCL_PIN);
  if (!mpu.setup(0x68)) {  // Change to 0x69 if the sensor's address is different
    Serial.println("MPU9250 connection failed");
    while (1);
  }
  previousTime = millis();
}

float alpha = 0.98; // Filter constant, adjust as needed
bool isExecuted = false;
```

```ino
void loop() {
  mpu.update();

  if (mpu.update()) {
    ax = mpu.getAccX() - accBias[0];
    ay = mpu.getAccY() - accBias[1];
    az = mpu.getAccZ() - accBias[2];

    unsigned long currentTime = millis();
    float deltaTime = (currentTime - previousTime) / 1000.0; // Convert time to seconds
    previousTime = currentTime;

    // Integrate acceleration to get velocity
    vx = alpha * (vx + ax * deltaTime) + (1 - alpha) * ax * deltaTime;
    vy = alpha * (vy + ay * deltaTime) + (1 - alpha) * ay * deltaTime;
    vz = alpha * (vz + az * deltaTime) + (1 - alpha) * az * deltaTime ;

    magAcc = sqrt(ax*ax+ay*ay+az*az)-0.98;
    magVel = sqrt(vx*vx+vy*vy+vz*vz);

    Serial.print(magAcc);
    Serial.print(",");
    Serial.println(magVel);


    delay(100); // Adjust the delay to match the desired sampling rate
  }
}
```

Şekil 5-33 Arduino IDE İle Yazılan İvmeölçer Kodu

Yukarıdaki şekilde gösterilen kodda görüldüğü gibi öncelikle sensörün ivmelenmedeki x, y ve z eksenlerindeki sapması (accBias) önceden sensor ile ölçülüp el ile girilmiştir. Ardından sensörden x, y ve z eksenlerindeki ivmelernme verileri elde edilip sonrasında tamamlayıcı filtre (complementary filter) kullanılarak hız verisi elde edilmiştir. Son olarakta ivmelenme ve hız verilerinin büyüklükleri hesaplanıp seri kanal ile gönderilmiştir. Seri kanal ile gönderilme nedeni sensor verisini ve GNSS alıcısından gelen verileri bilgisayar ortamına taşıyıp bu iki yerden gelen verileri bir ortamda birleştirmektir. Kod çalıştırıldığında çıktı olarak seri kanaldan ivmelenme verisinin büyüklüğünü ve hız verisinin büyüklüğünü virgül ile ayrılmış şekilde sürekli olarak verir.

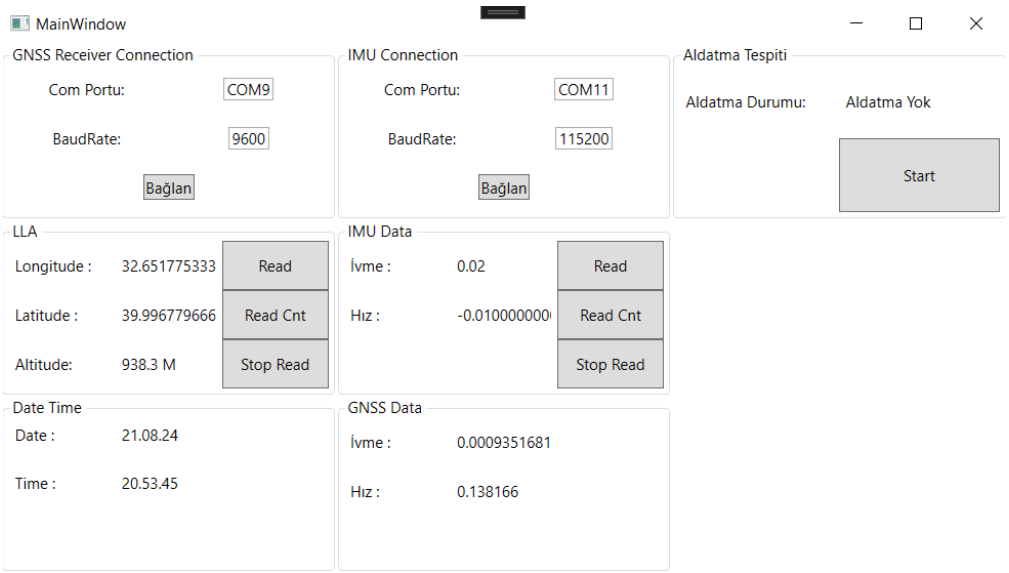
IMU sensöründen gelen veriler ile GNSS alıcısından gelen verileri birleştirmek için bilgisayar ortamında C# ile bir arayüz yazılmıştır. Bu arayüz ile hem GNSS alıcısından gelen konum, hız ve ivmelenme verileri hem de IMU sensöründen gelen ivmelenme ve hız verileri Şekil 5-34'te gözlenebilir.



Şekil 5-34 C# İle Yazılan Arayüz

Şekil 5-34 gösterilen arayüzde "IMU Data" grubunun altında bulunan İvme ve Hız verileri MPU9250 sensöründen gelen verileri; "GNSS Data" grubunun altında bulunan "İvme" ve "Hız" verileri GNSS alıcısından gelen verileri ifade eder. Arayüzü kullanmak için öncelikle "GNSS Receiver Connection" grubunun altında

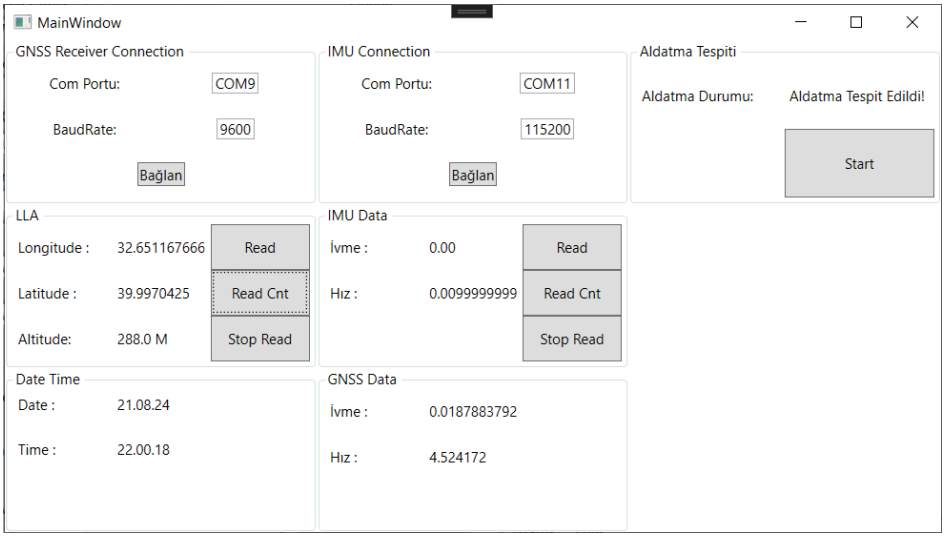
bulunan Bağlan butonuna tıklanılır ve “IMU Connection” grubunun altındaki “Bağlan” butonuna tıklanır. Ardından “LLA” grubunun altında bulunan “Read Cnt” butonuna ve “IMU Data” grubunun altında bulunan “Read Cnt” butonuna tıklanılır. Ardından arayüzde veriler görülmeye başlanır. Son olarak “Aldatma Tespiti” grubunun altında bulunan “Start” butonuna tıklanır ve Şekil 5-35’te gösterildiği gibi bir aldatma olduğunda tespit etmesi beklenir.



Şekil 5-35 GNSS Alıcısı Gerçek Konumu Aldıktan Sonra Arayüz Görüntüsü

Öncelikle GNSS alıcısının doğru konum alması sağlanır ve konum gözlemlenir. Ardından önceki başlıklarda yapılan aldatma saldırıları gibi GPS simülatöründen GPS sinyali yayılımı ve karıştırma sinyallerinin yayılımı yapılıp GNSS alıcısı aldatılmaya çalışılmıştır. Bu aldatma esnasında C# arayüzünden gözlemlenen veriler ile aldatma tespitinin yapılıp yapılmadığı gözlemlenmiştir. Aldatma saldırısı başladıktan sonra GNSS alıcısından gelen verilerde değişiklikler olduğu ve hız verisinin giderek arttığı gözlemlenmiştir. Ardından GNSS alıcısından gelen hız verisi ile IMU sensöründen hesaplanan hız verisi uyumsuzluğu arttıktan sonra C# arayüzünde ve Şekil 5-36’da görüldüğü gibi “Aldatma Tespit Edildi!” uyarısı gözlemlenebilir.

Bu çalışmadan da görülebileceği gibi GNSS alıcısı bir saldırıya maruz kaldığında GNSS sinyallerinden bağımsız ataletsel sensörler ile aldatma tespiti yapılabilir ve bu aldatma tespiti ile konumun güvenilirliği saptanabilir.



Şekil 5-36 Aldatma Saldırısı Tespitinden Sonra Arayüz Görüntüsü

6. SONUÇLAR

Bu tezde ilk olarak GNSS sistemleri, bu sistemlerde bulunan sinyaller, frekans bantları, kullanılan modülasyonlar incelenmiştir. Ardından bu sistemlerin sivil bileşenlerinin bilgileri halka açık olduğu için bu sistemleri çeşitli teknikler ile aldatmanın mümkün olabildiği düşünülmüştür. Bu yüzden GNSS sinyallerinin incelenmesinin ardından literatürde bulunan GNSS aldatma teknikleri incelenmiş ve bu aldatma teknikleri kullanılarak sivil alıcıları aldatma düşüncelerini de desteklemek için çeşitli deneysel çalışmalar yapılmıştır.

Bu deneysel çalışmalar ilk olarak sistemin kapalı bir ortamda yapılması şeklide başlamış ardından açık alanda çeşitli denemeler yapılmıştır. Kapalı ortamda yapılan denemelerde GNSS alıcıları ilk olarak aldatma sinyaline kilitlendiği ve gerçek uydu sinyalini alamadığı için sahte sinyaller ile konum çözümü yapıp yanlış konumu göstermiştir. Ayrıca sahte uydu sinyali ile hız verildiğinde alıcının hızı değişmiş ve bu şekilde de aldatılabilmiştir.

Ardından deneysel çalışmalar açık havada yapılmış ve öncelikle alıcıların açık havada gerçek uydu sinyali alması sağlanıp sonrasında sahte sinyal uygulanmıştır. Bu yöntemde de sadece GPS simülatörü bulunduğundan GPS sinyali yayını yapılmış fakat alıcı farklı uydulardan da veri aldığı için doğrudan aldatma gerçekleşmemiştir. Fakat GNSS alıcısının diğer frekans bantlarından aldığı sinyalleri karıştırıp simülatörden de GPS sinyali yayını yapılınca alıcının konumu kaybettiği ve simülatörden gelen sinyale kilitlendiği görülmüştür.

Aldatma saldırılarına karşı bir tedbir olan CRPA anten ile deneysel çalışmalara devam edilmiş ve bu çalışmalarda CRPA antenin içinde faz dizili antenleri ve sinyal işleme blokları olduğundan dolayı kolay bir şekilde aldatma sinyaline kilitlenmediği, anten konumlarının da bu aşamada önemli olduğu gözlemlenmiştir. Bu gözlem ile beraber anten konumları ayarlandıktan sonra CRPA anten ile kullanılan alıcı da karıştırma ve ardından aldatma saldırısı sonrasıda aldatılmıştır. Bu nedenle, aldatmaya karşı tam dayanıklı bir alıcı mimarisi oluşturmak için, GNSS sinyallerinden bağımsız olarak navigasyon verisi sağlayan bir ataletsel sensörün gerekli olduğu sonucuna varılmıştır. Bu doğrultuda, sisteme bir ivmeölçer sensörün entegre edilmesi gerektiği görülmüştür. Bu şekilde sensör verisi ile GNSS alıcısı verilerinin işlenip aldatma saldırılarına karşı ek bir güvenlik katmanı sağlaması ile

aldatma karşıtı bir alt sistem elde edilmiştir. Ardından uzun süreli aldatmalara tam dayanıklı bir mimari için çoklu sistem kullanılması gerektiği saptanmış ve aldatma karşıtı mimari ortaya çıkmıştır.

En az üç adet CRPA anten, GNSS alıcı ve aldatma dedektörünü içeren alıcı sistemi ile ve bu sistemlerden gelen verileri işleyen veri işleme ünitesi kullanılarak aldatma karşıtı bir mimari oluşturulmuş ardından deneysel çalışmalar ile bu mimari desteklenmiştir. Deneysel çalışmalarda ne kadar da CRPA antenli GNSS alıcısı aldatılmış olsa da gerçek saha koşullarında alıcının konumu iyi bir şekilde tespit edilemediğinden dolayı aldatıcı antenlerin konumlarının ayarlanması mümkün değildir. Ancak aldatıcı, alıcı konumunu tespit edip, aldatma saldırısını tespit edilen alıcı konumuna göre uygularsa (bu oldukça karmaşık bir aldatma saldırısı olur) sistemimizde bulunan ataletsel sensörler sayesinde aldatma saldırısı tespit edilmiş ve aldatma saldırısının başarılı olunduğu alt sistemden gelen verileri önemsemeden doğru konumu almaya devam edebiliriz. Bu elde edilen mimari aldatma karşıtı almaç mimarisi başlığı altında denklemler ve blok şemalar ile kapsamlı bir şekilde anlatılmış ve bu mimariye yönelik deneysel çalışmalar da şekiller ile detaylandırılmıştır.

7. KAYNAKLAR

[1] Jafarnia-Jahromi, Ali & Broumandan, Ali & Nielsen, J. & Lachapelle, Gérard. (2012). GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. International Journal of Navigation and Observation. 2012. 10.1155/2012/127072.

[2] M. L. Psiaki and T. E. Humphreys, “Protecting GPS from spoofers is critical to the future of navigation," IEEE Spectr., Jul. 2016.

[3] Misra, P. and Enge, P., 2006. Global Positioning System: Signals, Measurements, and Performance. 2nd ed. Ganga-Jamuna Press.

[4] Space Segment, https://www.gps.gov/systems/gps/space/, Erişim tarihi: **02.02.2024**

[5] GLONASS Space Segment, https://gssc.esa.int/navipedia/index.php/GLONASS_Space_Segment, Erişim tarihi: **02.02.2024**

[6] Control Segment, https://www.gps.gov/systems/gps/control/, Erişim tarihi: **02.02.2024**

[7] GLONASS Ground Segment, https://gssc.esa.int/navipedia/index.php?title=GLONASS_Ground_Segment, Erişim tarihi: **02.02.2024**

[8] The Navigation Message, https://www.e-education.psu.edu/geog862/node/1734, Erişim tarihi: **09.02.2024**

[9] Chinese BeiDou, https://www.e-education.psu.edu/geog862/node/1879, Erişim tarihi: **02.02.2024**

[10] C. Jiang, S. Chen, Y. Chen, Y. Bo, Q. Xia, and B. Zhang, “Analysis of the baseline data based GPS spoofing detection algorithm," in Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS), Monterey, CA, USA, Apr. 2018, pp. 397-403.

[11] G. Caparra, S. Ceccato, S. Sturaro, and N. Laurenti, “A key management architecture for GNSS open service navigation message authentication," in Proc. Eur. Navigat. Conf. (ENC), Lausanne, Switzerland, May 2017, pp. 287-297.

[12] D. Medina, C. Lass, E. P. Marcos, R. Ziebold, P. Closas and J. García, "On GNSS Jamming Threat from the Maritime Navigation Perspective," 2019 22th International Conference on Information Fusion (FUSION), Ottawa, ON, Canada, 2019, pp. 1-7, doi: 10.23919/FUSION43075.2019.9011348.

[13] GPS SPOOFING, https://powerofcommunity.net/poc2015/huang.pdf, Erişim tarihi: **09.02.2024**

[14] Z. Wu, Y. Zhang, Y. Yang, C. Liang and R. Liu, "Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey," in IEEE Access, vol. 8, pp. 165444-165496, 2020, doi: 10.1109/ACCESS.2020.3022294.

[15] L. Scott, “Anti-spoofing & authenticated signal architectures for civil navigation systems,'' in Proc. 16th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GPS/GNSS), Portland, OR, USA, Sep. 2003,pp. 1543-1552.

[16] M. L. Psiaki and T. E. Humphreys, “GNSS spoofing and detection,” Proc. IEEE, vol. 104, no. 6, pp. 1258-1270, Jun. 2016.

[17] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, “Assessing the spoofing threat,'' GPSWorld, vol. 20, no. 1,pp. 28-39, Jan. 2009.

[18] B. Dai, M. Xiao, and S. Huang, “GPS spoofing and inducing model of UAV,'' Commun. Technol., vol. 50, no. 3, pp. 496-501, Mar. 2017.

[19] L. He, W. Li, and C. Guo, “Study on GPS generated spoofing attacks,''Appl. Res. Comput., vol. 33, no. 8, pp. 2405-2408, Aug. 2016.

[20] M. Shi, S. Chen, H. Wu, and H. Mao, “A GPS spoofing pattern based on denial environment,'' J. Air Force Eng. Univ. (Natural Sci. Edition),vol. 16, no. 6, pp. 27-31, Dec. 2015.

[21] S. Huang, S. Chen, B. Yang, and H. Wu, “A power control strategy of multiple GNSS spoofing signals,'' J. Air Force Eng. Univ. (Natural Sci.Edition), vol. 18, no. 1, pp. 76-80, Feb. 2017.

[22] E. Schmidt, Z. Ruble, D. Akopian, and D. J. Pack, “Software-defned radio GNSS instrumentation for spoofing mitigation: A review and a case study,'' IEEE Trans. Instrum. Meas., vol. 68, no. 8, pp. 2768-2784,Aug. 2019.

[23] X. Xie, M. Lu, and D. Zeng, “Research on GNSS generating spoofing jamming technology," in Proc. IET Int. Radar Conf., Hangzhou, China, 2015, p. 5, doi: 10.1049/cp.2015.0999.

[24] H. Shen, “BeiDou-I satellite short message communication technology and application," Practical Electron., vol. 23, p. 106, 2014, doi: 10.3969/j.issn.1006-5059.2014.23.089.

[25] C. Wullems, O. Pozzobon, and K. Kubik, “Signal authentication and integrity schemes for next generation global navigation satellite systems," in Proc. Eur. Navigat. Conf. (GNSS), Munich, Germany, 2005, doi: 10.1049/ic:19970911.

[26] J. T. Curran and C. O'Driscoll, “Message authentication, channel coding & anti-spoofing," in Proc. 29th Int. Tech. Meeting Satell. Division The Inst. Navigat. (ION GNSS), Portland, OR, Sep. 2016, pp. 2948-2959.

[27] M. L. Psiaki and T. E. Humphreys, “GNSS spoofing and detection," Proc. IEEE, vol. 104, no. 6, pp. 12581270, Jun. 2016.

[28] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, ”An inline anti-spoofing device for legacy civil GPS receivers," in Proc.Int. Tech. Meeting The Inst. Navigat., San Diego, CA, Jan. 2010, pp. 698-712.

[29] Fruehauf, H., "A Better Way of Life for PPS Users...GPS SAASM and P(Y)-Direct, the New Wave of Military Receiver Technology for the PPS Navigation and Time and Frequency User," Proceedings of the 31th Annual Precise Time and Time Interval Systems and Applications Meeting, Dana Point, California, December 1999, pp. 347-356.

[30] Barker, Brian C., Betz, John W., Clark, John E., Correia, Jeffrey T., Gillis, James T., Lazar, Steven, Rehborn, Kaysi A., Straton, John R., "Overview of the GPS M Code Signal," Proceedings of the 2000 National Technical Meeting of The Institute of Navigation, Anaheim, CA, January 2000, pp. 542-549.

[31] SDRs for M-code satellite military communications, https://militaryembedded.com/comms/satellites/sdrs-for-m-code-satellite-military-communications, Erişim tarihi: **10.05.2024**

[32] Galileo Open Service Navigation Message Authentication,

https://gssc.esa.int/navipedia/index.php/Galileo_Open_Service_Navigation_Message_Authentication, Erişim tarihi: **10.05.2024**

[33] Galileo Open Service Navigation Message Authentication(OSNMA) SIGNAL-IN-SPACE INTERFACE CONTROL DOCUMENT (SIS ICD)

[34] A. Jovanovic, C. Botteron, and P.-A. Fariné, “Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers," in Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS), Monterey, CA, USA, May 2014, pp. 1258-1271.

[35] Boşnak, A. A. (2021). Uydu yörünge kontrol manevralarının çözümlemesi ve benzetimi (Yüksek lisans tezi, Hacettepe Üniversitesi).

[36] P. Papadimitratos and A. Jovanovic, "GNSS-based Positioning: Attacks and countermeasures," MILCOM 2008 - 2008 IEEE Military Communications Conference, San Diego, CA, USA, 2008, pp. 1-7, doi: 10.1109/MILCOM.2008.4753512.

[37] Inertial Navigation System (INS), https://support.sbg-systems.com/sc/kb/latest/integrated-motion-navigation-sensors/inertial-navigation-system-ins, Erişim tarihi: **11.05.2024**

[38] B. Kujur, S. Khanafseh and B. Pervan, "Experimental Validation of Optimal INS Monitor against GNSS Spoofer Tracking Error Detection," 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 2023, pp. 592-596, doi: 10.1109/PLANS53410.2023.10140096.

[39] Schmidt, George T.. “INS/GPS Technology Trends.” (2010).

[40] Gutierrez, P. (2023). Galileo HAS: A performance assessment in urban driving environments. Inside GNSS.

[41] USRP-2901 Specifications, https://www.ni.com/docs/en-US/bundle/usrp-2901-specs/page/specs.html?srsltid=AfmBOoqH1tOSgnGA6xW31vSxqSQpZykvCcwuJRRcVP3CA0p9qf1w1blD, Erişim tarihi: **10.05.2024**

[42] C099-F9P application board, https://www.u-blox.com/en/product/c099-f9p-application-board, Erişim tarihi: **03.06.2024**

[43] ANN-MB series, https://www.u-blox.com/en/product/ann-mb-series, Erişim tarihi: **15.03.2024**

[44] ANN-MB series, https://content.u-blox.com/sites/default/files/documents/ANN-MB_DataSheet_UBX-18049862.pdf, Erişim tarihi: **15.03.2024**

[45] TUALAJ 4200 MINI GPS/GNSS ANTI-JAM CRPA SYSTEM, https://www.tualcom.com/gps-gnss-anti-jam-crpa/tualaj-4200-mini/, Erişim tarihi: **14.05.2024**