T.C.

TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ YÜKSEK LİSANS PROGRAMI

MODERN JEODEZİK GNSS ALICILARININ KARIŞTIRMA DURUMUNDA KARARLILIĞI

YÜKSEK LİSANS TEZİ

Yasin YILDIRIM

Birinci Danışman: Doç. Dr. Levent GÖKREM

İkinci Danışman: Dr. Öğr. Üyesi Furkan KARLITEPE

TOKAT- 2025

ETİK SÖZLEŞME

Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim Enstitüsü tez yazım kılavuzuna göre, Doç. Dr. Levent GÖKREM danışmanlığında hazırlamış olduğum “Modern Jeodezik GNSS Alıcılarının Karıştırma Durumunda Kararlılığı” adlı Yüksek Lisans tezinin bilimsel etik değerlere ve kurallara uygun, özgün bir çalışma olduğunu, aksinin tespit edilmesi halinde her türlü yasal yaptırımı kabul edeceğimi beyan ederim.

16 / 07 / 2025

Yasin YILDIRIM

JÜRİ KABUL VE ONAY

Yasin YILDIRIM tarafından hazırlanan "**Modern Jeodezik GNSS Alıcılarının Karıştırma Durumunda Kararlılığı**" adlı tez çalışmasının savunma sınavı 16 / 07 / 2025 tarihinde yapılmış olup aşağıda verilen Jüri tarafından Oy Birliği ile Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim Enstitüsü Elektrik-Elektronik Mühendisliği Ana Bilim Dalı'nda Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Üyeleri **İmzası**

Üye (Başkan) :

Üye :

Üye :

ONAY

……./……./…….

Lisansüstü Eğitim Enstitüsü Müdürü

ÖZET

MODERN JEODEZİK GNSS ALICILARININ KARIŞTIRMA DURUMUMUNDA KARARLILIĞI

Yıldırım, Yasin
Yüksek Lisans, Elektrik-Elektronik Mühendisliği Bilim Dalı
Tez Danışmanı: Doç. Dr. Levent GÖKREM
II. Tez Danışmanı: Dr. Öğr. Üyesi Furkan KARLITEPE
Temmuz 2025, xi + 70 sayfa

Günümüzde konumlama ve yön bulma sistemleri çok önemlidir. Bu sistemler küresel uydu konumlandırma sistemleri (GNSS) olarak adlandırılmaktadır. GPS (ABD), GLONASS (Rusya), Galileo (Avrupa Birliği) ve BeiDou (Çin) kaynaklı temel uydu konumlama sistemleri olarak geçmektedir. Bu sistemler birçok alanda kullanılmaktadır. Bunlar bireysel yön bulma uygulamalarının yanı sıra savunma, ulaşım, enerji, tarım, inşaat, telekomünikasyon gibi birçok önemli sektörde aktif olarak kullanılmaktadır. Bu kadar geniş çaplı bir alanda kullanılan GNSS sistemlerinin güvenirliği de hali hazırda kritik bir öneme sahiptir.GNSS sistemleri zayıf sinyal yapısına sahip olması nedeniyle dışarıdan gelebilecek müdahalelere karşı savunmasızdır. Özellikle jamming (sinyal karıştırma) ve spoofing (sinyal aldatma) gibi saldırılar GNSS alıcılarının sinyali algılayamamasına veya yanlış konuma yönlendirme gibi olumsuz durumlara neden olmaktadır. Bu durum ciddi anlamda güvenlik riskleri oluşturabilmektedir. Özellikle askeri sistemler, insansız araçlar ve bu sistemin altyapısının kullanıldığı birçok alan için ciddi tehditler oluşturmaktadır.

Bu tez çalışmasında, GNSS sistemlerinin jamming ve spoofing saldırılarına karşı duyarlılığı deneysel olarak incelenmiştir. Deneysel çalışma kapsamında, Adalm Pluto ve HackRF One cihazları kullanılarak belirli mesafelerden GNSS sinyallerine sinyal karıştırma ve sinyal aldatma amacıyla müdahaleler gerçekleştirilmiş ve bu müdahalelerin konum doğruluğu üzerindeki etkileri analiz edilmiştir. Ayrıca Lora ve 2.4 GHz olmak üzere iki adet farklı anten kullanılarak antenlerin güçlerinin bu saldırılara etkileri gösterilmiştir. Hem statik hem de kinematik ölçüm senaryoları ile yürütülen testlerde; konum sapmaları, sinyal kalitesi, uydu takibi ve faz belirsizlikleri değerlendirilmiştir. Elde edilen bulgular, GNSS sistemlerinin dış sinyal tehditlerine karşı ne derece hassas olduğunu ortaya koymakta ve bu tür saldırılara karşı geliştirilecek savunma mekanizmaları için temel veri sağlanması amaçlanmaktadır.

Anahtar Kelimeler: GNSS, Jamming, Spoofing, Hassas Nokta Konumlandırma, SDR Algoritması, Gerçek Zamanlı Kinematik Konumlama

ABSTRACT

STABILITY OF MODERN GEODETIC GNSS RECEIVERS IN CASE OF JAMMING

Yıldırım, Yasin
Master's Thesis, Electrical-Electronic Engineering
Advisor: Asc. Prof. Dr. Levent GOKREM
II. Advisor: Asst. Prof. Dr. Furkan KARLITEPE
July 2025, xi +70 pages

Today, positioning and navigation systems play a vital role in numerous domains. These systems are known as Global Navigation Satellite Systems (GNSS). The main GNSS systems include GPS (USA), GLONASS (Russia), Galileo (European Union), and BeiDou (China). These systems are widely used not only in personal navigation applications but also in critical sectors such as defense, transportation, energy, agriculture, construction, and telecommunications. Given their extensive application areas, the reliability of GNSS systems is of critical importance. Due to the inherently weak structure of GNSS signals, these systems are highly vulnerable to external interferences. In particular, attacks such as jamming (signal interference) and spoofing (signal deception) can prevent GNSS receivers from detecting valid signals or can lead them to calculate false position data. These types of disruptions pose significant security threats, especially for military systems, unmanned vehicles, and other critical infrastructures that rely on GNSS-based services.

In this thesis, the vulnerability of GNSS systems to jamming and spoofing attacks is examined experimentally. Within the scope of the experimental study, GNSS signals were intentionally disrupted from specific distances using Adalm Pluto and HackRF One devices to simulate jamming and spoofing conditions, and the impacts of these interventions on positioning accuracy were analyzed. Additionally, two different types of antennas Lora and 2.4 GHz were used to observe how antenna strength affects system susceptibility to such attacks. Both static and kinematic measurement scenarios were tested, and variations in position accuracy, signal quality, satellite tracking, and phase ambiguities were evaluated. The results reveal the sensitivity of GNSS systems to external signal threats and aim to provide foundational data for the development of effective countermeasure strategies.

Keywords: GNSS, Jamming, Spoofing, Precise Point Positioning, SDR Algorithm, Real-Time Kinematic Positioning

TEŞEKKÜR

Yüksek lisans eğitimim boyunca tez çalışmamın başından sonuna kadar bana fikirleriyle, deneyimleriyle ve görüşleriyle yol gösteren kıymetli tez danışman hocalarım Doç Dr. Levent GÖKREM ve Dr. Öğr. Üyesi Furkan KARLITEPE'ye teşekkürlerimi sunarım.

Her anımda yanımda olan ve çalışmalarım boyunca desteklerini esirgemeyen çok değerli aileme teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR

Simgeler	Açıklamalar
dBm	Desibel-miliwatt
dB	Desibel
GHz	Gigahertz
MHz	Megahertz
Mbps	Saniye Başına Megabit
C/N_0	Sinyal-Gürültü Oranı
Db-Hz	Desibel-Hertz
Msps	Saniye Başına Megasamples
m	Metre
ns	Nanosaniye

Kısaltmalar	Açıklamalar
GNSS	Küresel Navigasyon Uydu Sistemleri
GPS	Küresel Konumlandırma Sistemi
RF	Radyo Frekansı
SDR	Yazılım Tanımlı Radyo
FM	Frekans Modülasyonu
İHA	İnsansız Hava Aracı
IMU	Ataletsel Ölçü Birimi
PRN	Sözde Rastgele Gürültü
DGPS	Ayrımsal Küresel Konumlama Sistemi
RTK	Gerçek Zamanlı Kinematik
SBAS	Uydu Tabanlı Arttırılmış Sistemler
WAAS	Geniş Alan Artırma Sistemi
EGNOS	Avrupa Jeostatik Navigasyon Kaplama Hizmeti
MSAS	Çok Fonksiyonlu Uydu Güçlendirme Sistemi
GAGAN	Hindistan Bölgesel Navigasyon Uydu Sistemi
PPP	Hassas Nokta Konumlandırması
DSP	Dijital Sinyal İşleme
AGC	Otomatik Kazanç Kontrolü
DOP	Hassasiyetin Seyreltilmesi
RAIM	Alıcı Otonom Bütünlük İzleme
SNR	Sinyal-Gürültü Oranı
DoA	Varış Yönü
ML	Makine Öğrenmesi
SVM	Destek Vektör Makineleri
IOT	Nesnelerin İnterneti
VSWR	Voltaj Duran Dalga Oranı
ADC	Analog-Dijital Çevirci
RINEX	Alıcıdan Bağımsız Değişim Formatı
NMEA	Ulusal Deniz Elektroniği Birliği
CBS	Coğrafi Bilgi Sistemleri
ZTD	Zenit Toplam Gecikme Değeri

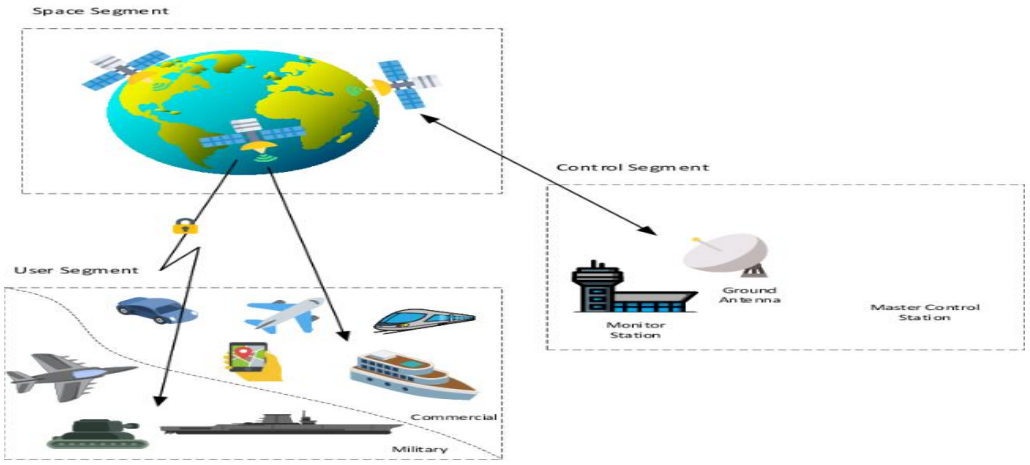
ŞEKİLLER LİSTESİ

ÇİZELGE LİSTESİ

1. GİRİŞ

Küresel Konumlandırma Sistemleri (GNSS – Global Navigation Satellite Systems), yeryüzündeki herhangi bir noktanın kesin konum bilgisini elde etmeyi sağlayan uydu tabanlı navigasyon sistemleridir. GNSS, temel olarak zaman ve konum bilgisi sağlayarak, birçok sektörde konum temelli olarak karar alma süreçlerinde kullanılmaktadır (Misra ve Enge, 2006). GPS (ABD), GLONASS (Rusya), Galileo (AB) ve BeiDou (Çin) gibi sistemler GNSS çatısı altında faaliyet göstermektedir.

GNSS teknolojileri, günümüzde yalnızca bireysel yön bulma uygulamalarıyla sınırlı kalmamakta aynı zamanda savunma sanayi, ulaştırma, tarım, enerji, inşaat, telekomünikasyon ve afet yönetimi gibi kritik alanlarda yaygın olarak kullanılmaktadır (Kaplan ve Hegarty, 2017). Özellikle askeri uygulamalarda hedefleme, izleme ve lojistik planlamada GNSS verilerinin yüksek hassasiyetli olması, operasyonel başarıyı doğrudan etkilemektedir. Bununla birlikte, GNSS sistemlerinin otonom kara ve hava araçlarında konumlandırma ve rota takibi gibi görevlerde vazgeçilmez bir rol üstlendiği bilinmektedir (Groves, 2014). Tarım sektöründe hassas tarım uygulamalarında traktörlerin otomatik yönlendirilmesi ve tohumlama gibi işlemler GNSS destekli olarak yürütülmekte; enerji sektöründe ise altyapı izleme, boru hattı güzergahları ve saha planlamaları bu sistemler aracılığıyla gerçekleştirilmektedir (Guo ve ark., 2018). Öte yandan, finans ve telekomünikasyon altyapıları da GNSS sistemlerinden elde edilen zaman senkronizasyon verilerine bağımlıdır. Örneğin, banka işlemlerinin doğru zaman etiketlemesi veya hücresel ağların koordinasyonu için GNSS tabanlı zaman bilgisi kritik öneme sahiptir (Jafarnia-Jahromi ve ark., 2012).



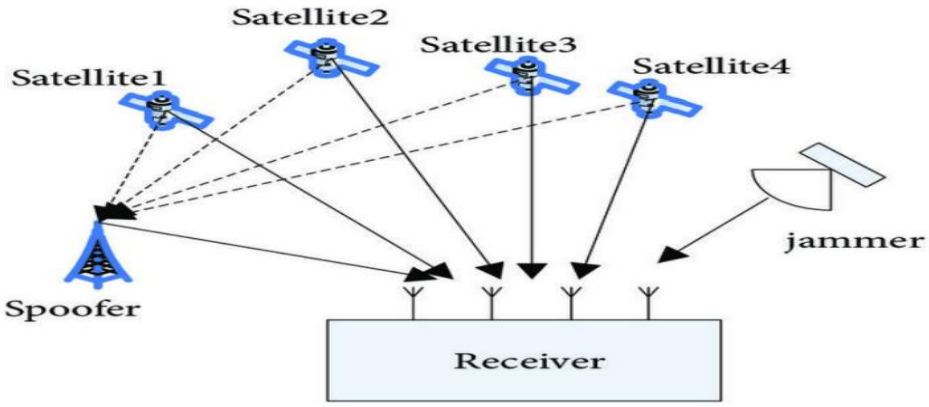
Şekil 1.1. GNSS uygulama sistemlerin havacılık, savunma, tarım, zamanlama gibi kullanım alanları

(Sanou, D. A. (2013).

GNSS sistemlerinin sağladığı bu geniş kapsamlı kullanım olanakları, aynı zamanda bu sistemlerin güvenliğini ve güvenilirliğini daha da önemli hale getirmektedir. Özellikle jamming (sinyal bozma) ve spoofing (sinyal aldatma) gibi tehditlerin artması, konum verisinin doğruluğunu ve sistem performansını riske atmakta ve bu alandaki güvenlik çalışmalarını öncelikli hale getirmektedir (Humphreys ve ark., 2008).

GNSS sistemlerinin sağladığı yüksek hassasiyetli konum, hız ve zaman bilgisi birçok sektörde vazgeçilmez hale gelmiş olsa da bu sistemlerin zayıf sinyal yapısı nedeniyle dış müdahalelere karşı savunmasız olduğu bilinmektedir (Psiaki ve Humphreys, 2016). GNSS sinyalleri, uydudan yeryüzüne doğru çok uzun bir mesafeyi kat ederek yalnızca -130 dBm mertebesinde bir güçle ulaşmakta, bu da onları elektromanyetik parazit ve kötü niyetli saldırılar açısından oldukça kırılgan hale getirmektedir (Wu ve ark. , 2020). Bu zayıflık, özellikle jamming ve spoofing gibi saldırı türlerinin GNSS güvenliği açısından ciddi tehditler oluşturmasına neden olmaktadır. Jamming saldırıları, ortamda GNSS sinyallerinden çok daha güçlü parazit sinyalleri üreterek alıcıların gerçek sinyali algılamasını engelleyen yöntemlerdir (Kerns ve ark., 2014). Bu tür saldırılar, genellikle düşük maliyetli RF jammer cihazları ile gerçekleştirilebilmekte ve konum servislerinin tamamen devre dışı kalmasına yol açabilmektedir.

Spoofing saldırıları ise daha sofistike olup, GNSS alıcısına sahte ama geçerli gibi görünen sinyaller gönderilerek cihazın yanlış konum bilgisi üretmesini sağlamayı hedefler (Humphreys ve ark., 2008). Bu saldırı türü, özellikle savunma, hava taşımacılığı ve finans gibi alanlarda yüksek risk barındırmaktadır. Spoofing sayesinde bir taşıtın yönü değiştirilebilir, bir drone hedefinden saptırılabilir veya zaman senkronizasyonuna dayalı sistemler manipüle edilebilir (Jafarnia-Jahromi ve ark., 2012).



Şekil 1.2. Aynı anda uygulanan hem jamming hem de spoofing saldırı senaryosu (Yang ve ark., 2019).

GNSS güvenliğini sağlamaya yönelik çeşitli yöntemler geliştirilmiş olsa da açık kaynaklı SDR (Yazılm tanımlı radyo) platformlarının yaygınlaşması, bu tür saldırıların daha kolay erişilebilir ve uygulanabilir hale gelmesine neden olmuştur. Özellikle Adalm Pluto, HackRF One gibi cihazlar yardımıyla düşük maliyetli ve taşınabilir jamming veya spoofing sistemleri kurulabilmekte; bu da sahada saldırıların uygulanabilirliğini artırmaktadır. Dolayısıyla, GNSS tabanlı sistemlerin güvenilirliğini sürdürebilmesi için bu tür tehditlerin sistematik olarak analiz edilmesi, etkilerinin ölçülmesi ve olası önlemlerin geliştirilmesi büyük önem taşımaktadır. Bu çalışmada da benzer şekilde, farklı mesafelerden gerçekleştirilen jamming ve spoofing saldırılarının GPS alıcısı üzerindeki etkileri deneysel olarak incelenmiştir.

Bu tez çalışmasının temel amacı, belirli mesafelerden gerçekleştirilen jamming ve spoofing müdahalelerinin, GPS alıcısından elde edilen konum doğruluğu üzerindeki etkilerini deneysel olarak analiz etmektir. Bu kapsamda, SDR teknolojileri kullanılarak gerçekleştirilen saldırıların, gerçek zamanlı konum verisine etkisi değerlendirilmiş ve bu etkiler mesafeye göre karşılaştırmalı olarak incelenmiştir. Ayrıca, saldırı sonrası oluşan sapma miktarları, konum kararlılığı ve sinyal kaybı gibi parametreler üzerinden analiz gerçekleştirilmiştir.

GNSS tabanlı sistemler, modern altyapıların kritik bir parçasını oluşturmakta ve savunma, ulaşım, telekomünikasyon, enerji ve finans gibi pek çok sektörde hayati roller üstlenmektedir (Kaplan ve Hegarty, 2017). Ancak, bu sistemlerin sinyal zayıflığı nedeniyle kötü niyetli saldırılara açık olması, özellikle jamming ve spoofing gibi tehditleri daha görünür hale getirmiştir (Psiaki ve Humphreys, 2016). Bu bağlamda yapılan bu çalışma, GNSS sinyallerinin zayıf noktalarını ortaya koyarak hem teknik hem de güvenlik açısından önemli katkılar sunmaktadır. Elde edilen bulgular, gelecekteki savunma mekanizmalarının tasarımına ve güvenli GNSS uygulamalarının geliştirilmesine yön verebilecek niteliktedir.

2. LİTERATÜR ÖZETİ

GNSS sistemleri savunma, telekomünikasyon, enerji gibi alanlarda çok kritik roller üstlenmektedir. Ancak bu sistemlerin sinyal zayıflığı durumundan ötürü bazı istenmeyen saldırılara açık konumdadır. Jamming ve spoofing gibi saldırı türleri bunlardan önemli olan bazı saldırı türleridir. Bu alanda yapılan çalışmalar GNSS sistemlerinin genel yapısına, güvenlik açıklarına, jamming ve spoofing saldırıları durumunda GNSS sinyallerinin tepkilerine odaklanmıştır. Tez çalışmasının bu bölümünde son yıllarda bu alanda yapılan çalışmalara yer verilmiştir.

Koca ve Ceylan (2018) tarafından yapılan çalışmada GNSS sistemlerinin güncel durumundan ve gelişmelerinden bahsetmiştir. GPS, GLONASS, Galileo ve Beidou gibi küresel uydu konumlama sistemlerinin teknik özelliklerini ve çalışma durumlarını karşılaştırmalı olarak inceleyip özetlemişlerdir. Koca ve Ceylan'ın derlemesi, her bir sistemin uydu sayısı, yörünge yapısı ve sinyal modernizasyonu gibi konularda teknik bir karşılaştırma sunarak GNSS alanındaki gelişmeleri aktarmaktadır.

Li ve arkadaşları (2023) tarafından yapılan bu çalışmada GNSS jamming tekniklerini bastırma karıştırması (geniş bantlı gürültü yayarak sinyali boğma) ve aldatma karıştırması (sinyalleri taklit ederek yanıltma) olarak iki ana kategoriye ayırmıştır. Yazarlar, karıştırma yöntemlerini sinyal türü, uygulanma aşaması ve zorluk derecesine göre sınıflandırıp her birinin etki değerlendirme ölçütlerini tartışmaktadır. Li ve ark.'nın çalışması, literatürdeki karıştırma verimliliğini değerlendirme metotlarını ve karıştırıcı cihazların konuşlanma stratejilerini de özetlemektedir. Bu derlemeye göre GNSS karıştırma, GNSS güvenliğine yönelik en yaygın tehditlerden biri haline gelmiştir ve son yıllarda basit bir FM vericisi veya ucuz SDR cihazıyla bile birkaç kilometrelik etki yarıçapına ulaşabilen karıştırma olayları rapor edilmiştir. Yazarlar, artan karıştırma vakalarına karşı anten sıralı düzenekleri, filtreleme ve işaret-gürültü izleme teknikleri gibi karşı önlemlerin de geliştiğini vurgulamaktadır.

Pavlovčič Prešeren ve arkadaşları (2021) yaptıkları çalışmada farklı türde GNSS alıcılarının doğruluk ve sinyal ölçümlerinin, değişik karıştırma senaryolarında nasıl etkilendiğini deneysel olarak analiz etmiştir. Yazarlar, chirp (süpürücü frekans) modülasyonlu bir karıştırıcı cihaz ile sabit ve hareketli karıştırma testleri yapmış; karıştırıcıyı alıcılardan farklı mesafelerde ve yükseklik farklarında konumlandırarak etkilerini gözlemlemiştir. Sonuçlar, güçlü bir karıştırma sinyalinin GNSS alıcılarındaki taşıyıcı-sinyal/gürültü oranını ani olarak 10 dB veya daha fazla düşürdüğünü ve bu düşüşün, alıcının doğrultu takibini bozarak konum çözümünde hatalara veya konum kaybına yol açtığını göstermektedir. Bu bulgular, GNSS alıcılarının karıştırıcı

sinyal modülasyonuna ve geometrik konumuna karşı hassasiyetini ortaya koymakta ve karıştırma tespit ve önleme tekniklerinin önemini vurgulamaktadır. Pavlovčič Prešeren ve arkadaşlarının yapmış olduğu çalışma bu tezde yapılan çalışma ile benzerlikler göstermektedir. Bu benzerlikler GNSS sistemine belirli mesafelerden jamming ve spoofing uygulama işlemi yönündendir.

Al-Soufi ve arkadaşları (2024) yaptıkları araştırmada insansız hava araçlarının (İHA) GPS'e bağımlılığı ve buna yönelik saldırılar deneysel olarak incelenmiştir. Yazarlar, bir HackRF One yazılım tanımlı radyo kullanarak bir ticari drone'a karşı GPS L1 ve L2 frekanslarında karıştırma ve spoofing saldırıları gerçekleştirmiş, ardından bu saldırılara karşı bir kurtarma yöntemi önermişlerdir. Karıştırma saldırılarında, drone'un GPS sinyali birkaç saniye içinde tamamen kesilerek cihazın konum bilgisini yitirdiği gözlenmiştir. Spoofing saldırılarında ise drone'a sahte GPS koordinatları beslenerek rotasından sapmasına yol açılmıştır. Çalışmanın önemli bir katkısı, geliştirilen **"**Return-to-Start**"** adlı otonom geri dönüş mekanizmasıdır. Bu mekanizma, bir saldırı tespit edildiğinde drone'un GPS alıcısını devre dışı bırakıp sadece ataletsel ölçüm birimi (IMU) verilerini kullanarak cihazı kalkış noktasına geri yönlendirmektedir. Bu çalışma, İHA'ların GNSS karıştırma ve aldatma saldırılarına karşı zaaflarını ve olası kurtarma çözümlerini ortaya koymaktadır.

Psiaki ve Humphreys (2016) tarafından yapılan çalışmada GNSS aldatma saldırılarının (spoofing) yöntemlerini ve savunma tekniklerini derinlemesine inceleyen bir çalışmadır. Yazarlar, sahte uydu sinyalleriyle alıcıları nasıl yanıltabileceğine dair pek çok senaryo tanımlamış ve literatürde öne çıkan karşı önlemleri özetlemiştir. Psiaki ve Humphreys'in çalışması, GNSS sahteciliğinin ciddiyetini ortaya koymuş ve takip eden yıllarda geliştirilecek tespit teknikleri için bir temel referans olmuştur.

Songala ve arkadaşları (2020) yaptıkları çalışmada akıllı telefon gibi kitle tüketimi GNSS alıcılarını aldatmanın ne kadar kolay olabileceğini göstermiştir. Yazarlar, düşük maliyetli bir yazılım tanımlı radyo (SDR) platformu kullanarak Android tabanlı bir akıllı telefonun GPS alıcısına sahte konum sinyalleri gönderip başarıyla yanlış konum raporlamasına neden olmuşlardır. Gerçekleştirilen basit spoofing senaryosunda, saldırgan cihaz telefonun yakınında bulunup gerçek GPS sinyalleriyle aynı frekansta fakat daha güçlü bir sahte GPS sinyali yaymıştır. Sonuçta telefon, gerçek uydu sinyallerini "gölgeleme" (overpower) yoluyla baskılayan bu sahte sinyallere kilitlenmiş ve kullanıcının konumunu birkaç yüz metre ötedeki bir izin verilen bölgeye taşınmış gibi göstermiştir. Bu çalışma, herhangi bir özel donanım geliştirmeden, sadece HackRF One gibi hazır bir SDR ve açık kaynaklı GPS sinyal jenerasyon

yazılımları ile aldatma saldırısının gerçekleştirilebildiğini ortaya koymuştur. Elde edilen bulgular, sivil GPS alıcılarının sinyal sahteciliğine karşı savunmasızlığını vurgulamaktadır.

Romaniuc ve arkadaşları (2025) tarafından yapılan çalışmada GNSS aldatma saldırılarının tespitine yönelik bu güncel çalışma, makine öğrenmesi tabanlı bir anomali tespit yöntemini önermektedir. Yazarlar, gerçek GNSS alıcılarından elde edilen gözlem verilerini kullanarak bir sinir ağı modelini eğitmiş ve bu modelin spoofing olaylarını normal durumdan ayırt etme performansını değerlendirmiştir. Çalışmada vurgulanan ana fikir, GNSS alıcı çıktısındaki parametrelerin (taşıyıcı-genlik, pseudorange, sinyal gücü vs.) zaman içindeki davranışının öğrenilerek beklenmedik anomalilerin tespit edilmesidir. Bu çalışma ayrıca GNSS güvenliğinde çoklu-frekanslı ve çoklu-parametreli analizlerin önemine dikkat çekmektedir. Tek frekanstan tek bir ölçüte bakarak yapılan tespitlerin yetersiz kalabildiği bunun yerine yapay öğrenme modellerinin aynı anda birden fazla sinyal özelliğini değerlendirmesinin daha güvenilir sonuçlar verdiği gösterilmiştir. Sonuç olarak Romaniuc ve arkadaşları, GNSS aldatma tespitinde veri odaklı yaklaşımların etkinliğini kanıtlamakta ve gelecekte gerçek zamanlı uygulanabilirlik için bu tür modellerin donanım seviyesinde optimize edilebileceğini önermektedir.

Wang ve arkadaşları (2021) yaptıkları çalışmada , GNSS spoofing tespitinde son yıllarda öne çıkan Radyo Frekansı Parmakizi (RF fingerprinting) yöntemlerini kapsamlı bir şekilde ele almaktadır. Bu derlemeye göre RF parmakizi yöntemleri henüz gelişme aşamasında olsa da, GNSS aldatmasını tespit için ilave bir katman sağlayarak mevcut koruma tekniklerini tamamlayıcı bir rol oynayabilir. Wang ve arkadaşları, gelecekte farklı coğrafi bölgelerden toplanacak geniş ham veri setleriyle eğitilecek makine öğrenimi modellerinin, sahte sinyalleri küresel ölçekte neredeyse gerçek zamanlı tanıyabilecek bir izleme ağı oluşturabileceğini öngörmektedir.

Radoš ve arkadaşları (2024) tarafından yapılan çalışmada , GNSS karıştırma ve aldatma saldırılarının tespit yöntemlerini sistematik bir şekilde incelemiş ve literatürdeki boşluklara dikkat çekmiştir. Yazarlar, şimdiye kadar yayınlanan çalışmaların çoğunun karıştırma ve aldatma tehditlerini ayrı ayrı ele aldığını, oysa gerçek hayatta bu iki tehdidin birleşik olarak ortaya çıkmasının tespitini sağlamanın kritik fakat ihmal edilmiş bir konu olduğunu belirtmektedir. Makalede, “ikili girişim (dual interference)” olarak adlandırılan eşzamanlı jamming+spoofing senaryolarının tespitine dair çok az sayıda çalışma olduğu vurgulanmıştır.

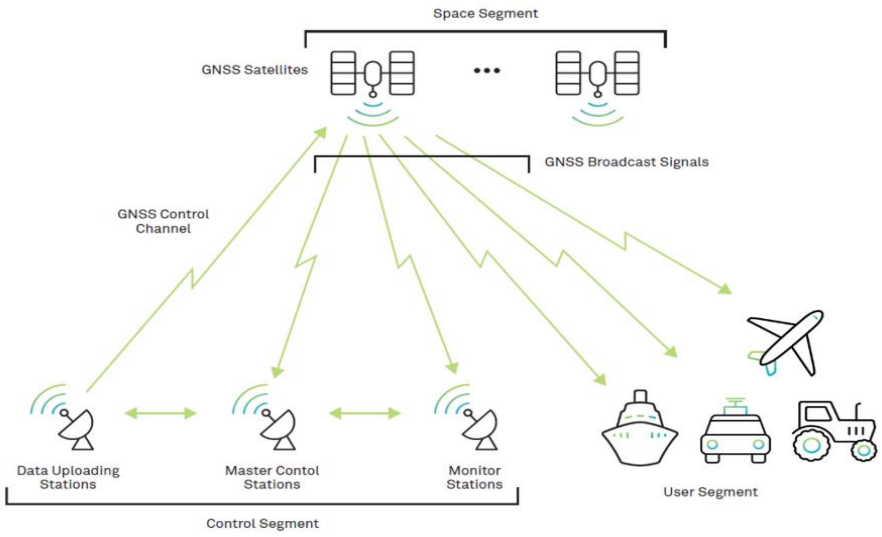
Radoš ve arkadaşları (2024) yaptıkları çalışmanın işaret ettiği diğer bir nokta da açık erişimli veri setlerinin ve standardize test senaryolarının eksikliğidir. Akademik araştırmacılar, gerçek jamming ve spoofing olaylarını yeniden üretip tespit algoritmalarını doğrulayacak veri sıkıntısı çekmektedir. Bu durum, literatürde saldırgan-alıcı mesafesi, saldırı gücü ve senaryo çeşitliliği açılarından kapsamlı analizler yapılmasını sınırlamıştır. Radoš ve ark., ileriki araştırmalar için farklı koşulları içeren zengin veri kümelerinin oluşturulmasını ve paylaşılmasını önermektedir. Bu bağlamda, literatürdeki boşlukların doldurulması, GNSS tabanlı kritik sistemlerin güvenliği için acil bir ihtiyaç olarak belirtilmiştir.

3. KURAMSAL TEMELLER

3.1. GNSS Sistemleri

Küresel Uydu Seyrüsefer Sistemleri (GNSS), uydular, yer kontrol istasyonları ve kullanıcı alıcıları arasındaki etkileşim aracılığıyla dünya üzerindeki herhangi bir noktanın konum, zaman ve hız bilgisini sağlayan uzay tabanlı navigasyon sistemleridir. Bu sistemler, kullanıcıların bağımsız veya birlikte çalışabilen çoklu sistemler üzerinden konumlandırma yapmasına olanak tanır. Mevcut temel GNSS sistemleri arasında GPS (ABD), GLONASS (Rusya), Galileo (Avrupa Birliği) ve BeiDou (Çin) yer almaktadır. Bu sistemler, kullanıcı alıcılarına sürekli ve küresel kapsamlı hizmet sağlayarak başta savunma, sivil havacılık, ulaşım, tarım ve telekomünikasyon olmak üzere pek çok alanda kritik rol oynamaktadır (Teunissen ve Montenbruck, 2017).

GNSS sistemlerinin çalışma prensibi; uydulardan yayılan sinyallerin, yeryüzündeki alıcı tarafından alınması ve bu sinyallerin gönderim zamanları ile alınma zamanları arasındaki farktan pseudorange (sözde mesafe) hesaplanması esasına dayanır. En az dört farklı uydudan alınan sinyallerle alıcının üç boyutlu konumu ve saat düzeltmesi belirlenebilir. Bu işlem, trilaterasyon yöntemi ile gerçekleştirilir (Pica ve ark., 2022).



Şekil 3.1. GNSS sistemlerinin uzay, kontrol ve kullanıcı segmentleri

(NovAtel, 2021).

3.1.1. GNSS sinyal yapısı ve frekanslar

GNSS uyduları, taşıyıcı frekanslar üzerine kodlanmış sinyaller yayınlar. Bu sinyallerin temel bileşenleri şunlardır: Taşıyıcı dalga, pseudorandom noise (PRN) kodları ve navigasyon mesajıdır.

3.1.2. Taşıyıcı dalga ve frekanslar

Taşıyıcı dalga, veri taşımak için kullanılan yüksek frekanslı elektromanyetik dalgadır. GNSS sistemlerinde en yaygın kullanılan frekans bantları, L bandı içinde yer alır (1–2 GHz aralığı). Örneğin GPS sistemi, aşağıdaki taşıyıcı frekansları kullanır:

- L1 bandı: 1575.42 MHz – sivil kullanıcılar için temel taşıyıcıdır.
- L2 bandı: 1227.60 MHz – askeri sinyaller ve gelişmiş uygulamalar (ör. diferansiyel GPS) için kullanılır.
- L5 bandı**:** 1176.45 MHz – yüksek doğruluk ve parazit bağışıklığı sunan yeni nesil sivil sinyaldir.

Bu frekansların kullanımı sayesinde çoklu frekanslı GNSS alıcıları iyonosferik gecikmeleri düzeltebilir ve daha hassas konum hesaplaması yapabilir (Yang ve ark., 2025).

3.1.3. Kod yapısı

GNSS sinyalleri, her bir uyduya özgü PRN kodlarıyla modüle edilmiştir. Bu kodlar sayesinde alıcı, hangi sinyalin hangi uyduya ait olduğunu ayırt edebilir. GPS sisteminde kullanılan kod türleri şunlardır:

- C/A (Coarse/Acquisition) kodu: L1 frekansı üzerine modüle edilmiş olup sivil kullanıcılar için tasarlanmıştır. 1.023 Mbps hızında yayınlanır ve alıcının hızlı sinyal yakalamasına olanak tanır.
- P(Y) kodu: L1 ve L2 frekansları üzerine modüle edilmiş, şifreli ve genellikle askeri kullanım içindir. 10.23 Mbps hızındadır.
- M kodu**:** GPS Modernizasyon Projesi kapsamında geliştirilen ve daha yüksek güvenlikli kullanım için planlanan sinyaldir.

Galileo, BeiDou gibi sistemlerde de benzer şekilde hem açık hem de kontrollü erişim sinyalleri bulunmakta; çoklu frekanslarda PRN ve alt taşıyıcı kodlama yapıları kullanılmaktadır (Xue ve ark., 2022).

3.1.4. Navigasyon mesajı

Taşıyıcı dalga üzerine gömülü olarak iletilen navigasyon mesajları, uydu yörünge bilgilerini, saat düzeltmelerini ve sistem durum bilgilerini içerir. Bu mesajlar sayesinde GNSS alıcısı uyduların tam konumunu ve sinyalin gönderildiği zamanı öğrenerek konum hesaplamasını gerçekleştirir (Chen ve ark., 2013).

3.2. GNSS Konum Belirleme Türleri

GNSS sistemleri, kullanıcıya konum, hız ve zaman bilgisi sunarken farklı düzeylerde doğruluk ve güvenilirlik sağlayan çeşitli konum belirleme yöntemleri sunar. Bu yöntemler; kullanılan uydu sayısı, ölçüm tekniği, düzeltme verilerinin varlığı ve alıcının özelliklerine bağlı olarak değişkenlik gösterir. GNSS konum belirleme türleri genel olarak rölatif, mutlak (stand-alone), diferansiyel (DGPS), RTK (gerçek zamanlı kinematik), SBAS (uydu tabanlı artırılmış sistemler) ve ağ destekli yöntemler gibi sınıflarda incelenebilir (Hoffmann-Wellenhof ve ark., 2008; Leick ve ark., 2015).

3.2.1 Rölatif konum belirleme

Rölatif konum belirleme, iki veya daha fazla GNSS alıcısı arasındaki konum farkının belirlenmesine dayalı bir yöntemdir. Bu teknikte, biri referans (baz) istasyonu olarak sabitlenen, diğeri ise hareketli alıcı olan iki GNSS cihazı kullanılır. Referans alıcısının konumu hassas biçimde bilindiğinden, bilinmeyen alıcının konumu bu referans noktasına göre yüksek doğrulukla hesaplanabilmektedir (Leick et al., 2015). Rölatif konum belirlemede, her iki alıcının aynı anda aynı uydulardan gelen sinyalleri gözlemlemesi esas alınır. Bu eşzamanlı gözlemler sayesinde, iyonosferik ve troposferik gecikmeler, uydu saat hataları gibi ortak hata bileşenleri büyük oranda ortadan kaldırılabilir. Bu sayede milimetre düzeyinde hassasiyet sağlanabilmektedir. Özellikle gerçek zamanlı kinematik (RTK) ve post-processing kinematik (PPK) gibi uygulamalarda rölatif konumlandırma tekniği sıklıkla kullanılmaktadır (Hofmann-Wellenhof et al., 2008). Rölatif konum belirleme, tek frekanslı sistemlerde kısa baz çizgiler (genellikle <10 km) için yeterli doğruluk sağlarken, çift frekanslı GNSS alıcıları ile bu mesafe daha da artırılabilir. Ayrıca taşıyıcı faz ölçümlerinin kullanılması ile birlikte konum doğruluğu önemli ölçüde yükselmektedir. Bununla birlikte, faz belirsizliğinin çözülmesi, uydu görünürlüğü ve baz uzunluğu gibi faktörler sistemin başarımını doğrudan etkilemektedir (Teunissen & Montenbruck, 2017).

3.2.2. Mutlak konum belirleme (Stand-alone positioning)

Bu yöntem, GNSS alıcısının yalnızca uydulardan aldığı sinyalleri kullanarak konum belirlemesidir. Düzeltme verisi olmaksızın yapılan bu çözümlemede, alıcının doğruluğu genellikle 3–10 metre aralığındadır. En az dört uydudan gelen sinyalle, alıcının x, y, z koordinatları ve saat farkı hesaplanır. Sivil kullanımda en yaygın yöntemlerden biridir, ancak hata kaynaklarına karşı duyarlıdır (Teunissen ve Montenbruck, 2017).

3.2.3. Diferansiyel GNSS (DGPS)

DGPS, referans istasyonları aracılığıyla GNSS sinyallerindeki hataların modellenip, mobil kullanıcılara düzeltme verisi gönderilmesine dayalı bir yöntemdir. Referans istasyonu, konumu bilinen sabit bir alıcıdır ve gerçek konumu ile GNSS'ten hesaplanan konumu arasındaki farkı belirleyerek düzeltme sinyali üretir. Bu düzeltme, yakın çevredeki mobil alıcılar tarafından uygulandığında konum doğruluğu 1–3 metreye kadar artırılabilir (U.S. Coast Guard, 2020).

3.2.4. Gerçek zamanlı kinematik (RTK) konumlama

RTK, taşıyıcı faz ölçümlerine dayalı yüksek hassasiyetli bir konumlama yöntemidir. Sabit bir referans istasyonu ile hareketli bir alıcı arasında gerçek zamanlı veri alışverişi sağlanır ve faz farkı ölçümleri kullanılarak birkaç santimetre seviyesinde konum doğruluğu elde edilir. Özellikle mühendislik uygulamaları, tarım, haritalama ve insansız hava araçlarında yaygın olarak kullanılmaktadır (Wanninger, 2003). RTK sistemleri; taşıyıcı faz çözümlemeye dayalı oldukları için yüksek doğruluk sunsalar da, baz istasyonuna olan uzaklık arttıkça hassasiyet azalır ve iletişim altyapısına (LoRa ve GSM gibi) gereksinim duyarlar.

3.2.5. Uydu tabanlı artırılmış sistemler (SBAS)

SBAS, GNSS sinyallerindeki hataları düzeltmek amacıyla bölgesel düzeyde faaliyet gösteren, uydu destekli sistemlerdir. ABD'de WAAS, Avrupa'da EGNOS, Japonya'da MSAS, Hindistan'da GAGAN gibi sistemler bu kategoriye girer. Yer tabanlı izleme istasyonları, uydu sinyallerindeki hataları analiz ederek düzeltme verisi üretir ve bu veriler, geostatik uydular aracılığıyla GNSS kullanıcılarına iletilir. Bu yöntemle doğruluk 1–2 metre seviyesine kadar artırılabilir (Eurocontrol, 2021).

3.2.6. Ağ tabanlı konumlama yöntemleri (Network-RTK, PPP)

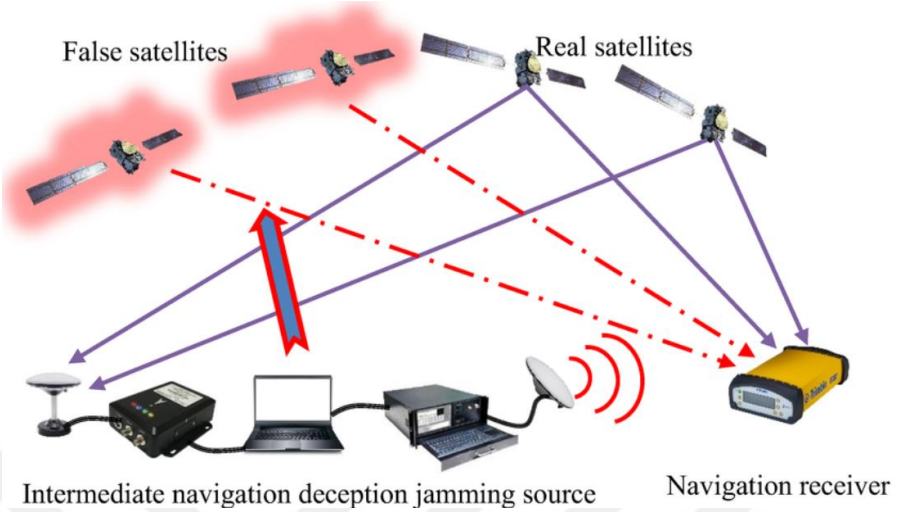
Network RTK, birden fazla referans istasyonundan alınan verilerin ağ merkezinde işlenerek kullanıcıya gönderildiği yöntemdir. Geniş alanlarda, klasik RTK'ya göre daha istikrarlı sonuçlar sağlar.

PPP (Precise Point Positioning) yöntemi ise GNSS uydularının yörünge ve saat hatalarını içeren hassas ürünlerin kullanılmasıyla alıcının konumunu metre-altı hassasiyetle çözümlemesini sağlar. PPP, düzeltme verilerini genellikle internet üzerinden alır ve dünya çapında uygulama imkânı sunar (Zumberge ve ark., 1997).

3.3. Jamming Kavramı ve Türleri

Jamming, GNSS sistemlerine yönelik olarak gerçekleştirilen, kasıtlı elektromanyetik sinyallerle alıcının gerçek uydu sinyallerini alamamasına neden olan bir saldırı türüdür. Bu saldırılar, GNSS alıcısının sinyal alımını tamamen engelleyebilir veya ciddi ölçüde bozarak

konum, zaman ve hız hesaplamalarında büyük hatalara neden olabilir (Gao ve ark., 2012). GNSS sinyallerinin zayıf doğası nedeniyle, düşük güçlü bir parazit sinyali bile alıcının performansını önemli ölçüde etkileyebilir (Akos, 2012).



Şekil 3.2. GNSS jamming işlemi şeması

(Li ve ark., 2023)

3.3.1 Gürültü temelli jamming (Noise-based jamming)

Gürültü temelli jamming, geniş bantlı veya dar bantlı rastgele elektromanyetik sinyallerin GNSS frekans aralıklarına gönderilmesi ile gerçekleştirilir. Bu tür saldırılarda genellikle white noise (beyaz gürültü) üreten RF kaynakları kullanılır. Özellikle L1 (1575.42 MHz) ve L2 (1227.60 MHz) taşıyıcı frekanslarına yöneltilen yüksek güçlü gürültüler, GNSS alıcısının Taşıyıcı-Gürültü Oranı (C/N_0) değerini düşürerek sinyalin çözülmesini zorlaştırır veya imkânsız hale getirir (Lo ve Enge, 2011). Geniş bantlı gürültü jammer'ları genellikle tüm GNSS sinyal spektrumunu hedef alır, bu da sivil alıcılarda ciddi veri kayıplarına yol açabilir.

3.3.2. Sweep jamming

Sweep jamming, belirli bir frekans aralığında sistematik olarak ileri-geri süpürme yapan dar bantlı bir jamming türüdür. Bu yöntem, geniş bir frekans aralığını sırayla hedef alarak alıcının frekans tarama ve filtreleme yeteneklerini aşmayı amaçlar (Kerns ve ark., 2014). GNSS sistemlerinde bu tür saldırılar, zaman içinde hem L1 hem de L2 sinyallerini etkileyebilir. Sweep jammerların başarısı, tarama hızı ve güç seviyesine bağlıdır. Hızlı sweep sinyalleri, özellikle zaman tabanlı filtreleme kullanan alıcılar için tehlikeli olabilir çünkü her frekans diliminde kısa ama yıkıcı bir etki yaratırlar.

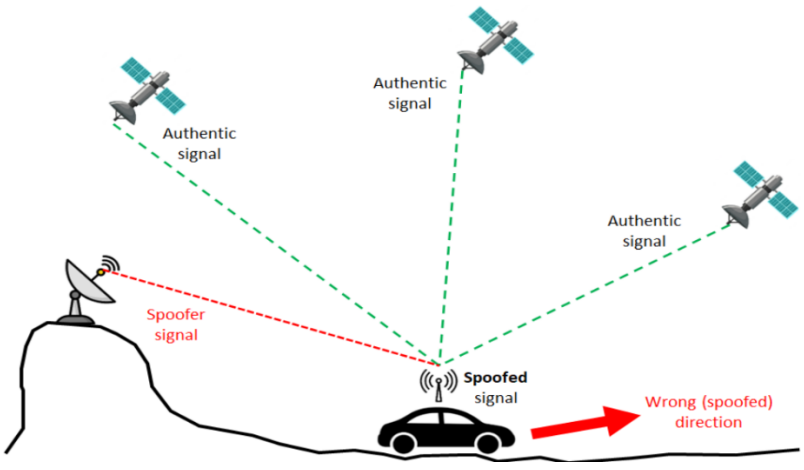
3.3.3. Tone jamming

Tone jamming, sabit frekansta veya dar frekans aralığında yüksek güçlü saf sinüzoidal sinyallerin iletilmesiyle gerçekleştirilir. Bu yöntem genellikle düşük bant genişliğinde enerji yoğunluğu sağlayarak, GNSS taşıyıcı sinyalleriyle doğrudan çakışma yaratır (Tanil ve ark., 2018). Tek tonlu jamming, bir taşıyıcı frekansı hedef alırken; çok tonlu (multi-tone) jamming, aynı anda birden fazla GNSS sinyalini bastırmayı amaçlayabilir. Özellikle DSP (Dijital Sinyal İşleme) tabanlı alıcılarda, taşıyıcı sinyalin içeriği çarpıtılarak takip algoritmaları sekteye uğratılır.Tone jamming'in diğer yöntemlere kıyasla avantajı, düşük güçle bile etkili olabilmesi; ancak dezavantajı, tespiti nispeten kolay olan dar bantlı bir spektruma sahip olmasıdır. Bu nedenle, askeri uygulamalarda genellikle gürültü ve ton jamming birlikte kullanılmaktadır.

3.4. Spoofing Kavramı ve Yöntemleri

Spoofing, GNSS sistemlerine yönelik sofistike bir saldırı türü olup, alıcıyı sahte ancak geçerli gibi görünen GNSS sinyalleriyle yanıltarak yanlış konum, hız veya zaman bilgisi üretmesini sağlamayı hedefler. Bu saldırı türünde, saldırgan; gerçek uydulara benzer yapıda ve genellikle daha güçlü sinyaller göndererek GNSS alıcısının sahte sinyallere kilitlenmesini sağlar. Böylece, alıcı cihazın çıktısı manipüle edilirken kullanıcı sisteminin bunu algılaması çoğu zaman mümkün olmaz (Tippenhauer ve ark., 2011).

GNSS spoofing, jamming'e kıyasla daha karmaşık ve etkili bir saldırı biçimidir çünkü sadece alıcıyı işlevsiz hale getirmekle kalmaz, aynı zamanda onu bilinçli olarak hatalı veri üretmeye yönlendirir. Bu nedenle, hava ve kara araçları, otonom sistemler, zaman senkronizasyon altyapıları ve güvenlik tabanlı uygulamalar açısından ciddi tehditler barındırmaktadır (Psiaki ve Humphreys, 2016).



Şekil 3.3. Spoofing saldırısının süreçsel etkisi

(Liu ve ark., 2018)

3.4.1. Tekrarlayıcı (Replay) spoofing

Bu yöntemde saldırgan, daha önce alınmış gerçek GNSS sinyallerini kaydeder ve daha sonra bu sinyalleri gecikmeli biçimde yeniden yayar. Bu sayede alıcı, sinyalin geç geldiğini varsayarak yanlış konum hesaplaması yapar. Replay saldırıları, görece düşük karmaşıklığa sahip olup, özellikle hareketli hedeflerin yönünün değiştirilmesi gibi uygulamalarda kullanılır (Magiera ve Katulski, 2016). Ancak sinyalin yalnızca tekrarı söz konusu olduğundan hedef alıcıyı daha uzun süre kandırmak zordur.

3.4.2. Senkronsuz yazılım tabanlı spoofing

Bu yöntemde, yazılım tabanlı sinyal üreticileri ile GNSS sinyalleri sıfırdan simüle edilir. Saldırgan, sahte uydulara ait sinyalleri doğrudan yazılım ile oluşturur ve SDR cihazı aracılığıyla yayar. En çok kullanılan açık kaynaklı araçlardan biri olan GPS-SDR-SIM, bu tür saldırılar için temel platformlardan biridir (Burbank ve ark., 2024). Senkronsuz spoofing'in başarılı olabilmesi için sahte sinyallerin gerçek sinyallerle örtüşecek kadar benzer olması gerekir. Aksi halde alıcı cihaz senkronizasyon hatası nedeniyle sinyali reddedebilir.

3.4.3. Senkronize yazılım tabanlı spoofing (Intermediate-level spoofing)

Bu yöntemde sahte sinyaller, gerçek GNSS sinyalleriyle zaman, frekans ve kod fazı bakımından senkronize olacak şekilde üretilir. Alıcı bu geçişi fark etmeden sahte sinyallere kilitlenir. Bu tür saldırılar genellikle **"**carry-off" stratejisi olarak adlandırılır; alıcı önce doğru konumu gösterir, sonra yavaşça sahte konuma sürüklenir. Bu geçiş yumuşak olduğu için fark edilmesi güçtür (Bhatti ve Humphreys, 2017).

3.4.4. Çoklu taşıyıcı frekanslı (Multifrequency) ve MIMO tabanlı spoofing

Son yıllarda literatürde, birden fazla taşıyıcı frekans (örneğin L1 + L2 + L5) üzerinde eş zamanlı spoofing gerçekleştiren sofistike senaryolar raporlanmıştır. Bu tekniklerde çoklu anten ve faz ayarlı sinyal üretimi (beamforming) gibi yöntemler kullanılarak hedef GNSS alıcısının daha hassas aldatılması amaçlanır (Egea-Roca ve ark., 2022). Özellikle askeri sınıf sistemlerde, bu tür saldırıların etkili olabileceği vurgulanmaktadır.

Spoofing saldırılarının yaygınlaşmasında en büyük etkenlerden biri, düşük maliyetli SDR cihazlarının (örn. HackRF One, USRP, BladeRF) ve açık kaynaklı sinyal üretim yazılımlarının yaygınlaşmasıdır. Bu donanımlar sayesinde, teknik bilgisi sınırlı kişiler dahi saldırı gerçekleştirebilir duruma gelmiştir. Özellikle HackRF One gibi cihazlar ile düşük güçlü ve taşınabilir spoofing sistemleri kolayca inşa edilebilmektedir (Kerns ve ark., 2014).

3.5. Sinyal Bozunum ve Konum Hesaplaması İlişkisi

GNSS sistemlerinin doğruluğu, güvenilirliği ve sürekliliği; alınan sinyallerin kalitesi ile doğrudan ilişkilidir. Sinyal kalitesinde meydana gelen bozulmalar, konum hesaplamalarının hassasiyetini olumsuz yönde etkileyebilir. Bu bağlamda, taşıyıcı-gürültü Oranı (Carrier-to-Noise Ratio – C/N_0), pseudorange (sözde mesafe) ve konum doğruluğu arasındaki ilişki, GNSS performansını değerlendirmede temel parametreler arasında yer alır (van Diggelen, 2009).

3.5.1. Taşıyıcı-gürültü oranı (C/N_0)

C/N_0, alıcının aldığı taşıyıcı sinyal gücü ile termal gürültü seviyesi arasındaki oranı ifade eder ve genellikle dB-Hz birimiyle gösterilir. GNSS sinyallerinin düşük güçlü (~–130 dBm) yapısı nedeniyle bu oran genellikle 30–50 dB-Hz aralığında değişir. Yüksek C/N_0 değeri, sinyalin gürültüye karşı güçlü olduğunu ve alıcının sinyali sağlıklı bir şekilde çözümleyebildiğini gösterir (Kaplan & Hegarty, 2017). C/N_0 değeri düşmeye başladığında, alıcının hem kod hem de taşıyıcı faz çözümlemesi zorlaşır; bu da doğrudan konum doğruluğunu olumsuz etkiler.

Bozunum senaryolarında (örneğin jamming veya atmosferik bozulmalar), C/N_0 değeri hızla düşer. Eğer bu oran 25 dB-Hz altına inerse, çoğu alıcı konum çözümünü sürdüremez veya sinyali kaybeder. Ayrıca, alıcının otomatik kazanç kontrolü (AGC) gibi iç parametreleri de bu düşüşten etkilenerek hatalı konum üretimine neden olabilir (Han ve ark., 2016).

3.5.2. Pseudorange (Sözde mesafe)

Pseudorange, GNSS uydusu ile alıcı arasındaki mesafenin, sinyalin gönderim ve alınma zamanları arasındaki farkın ışık hızı ile çarpılması sonucu elde edilen değerdir. Bu mesafe, aslında "gerçek" mesafeden farklıdır çünkü içinde uydu saat hatası, alıcı saat hatası, atmosferik gecikme (iyonosfer, troposfer), çoklu yol (multipath) etkisi gibi pek çok bileşeni barındırır (Misra ve Enge, 2006). Pseudorange hesaplamaları ne kadar hassas olursa, alıcının konum çözümlemesi de o denli doğru olur.

Sinyal bozulduğunda örneğin spoofing etkisiyle alıcı yanlış zaman damgası içeren sahte sinyallere kilitlenir ve buna bağlı olarak hesaplanan pseudorange değerleri sapar. Bu sapmalar genellikle birkaç metre ile sınırlı olabilirken, bazı durumlarda kilometre düzeyinde konum hatalarına yol açabilir (Jafarnia-Jahromi ve ark., 2012).

3.5.3. Konum doğruluğu üzerindeki etki

GNSS sistemlerinde konum doğruluğu; uydu geometrisi, sinyal kalitesi ve hata kaynaklarının büyüklüğüne bağlı olarak değişkenlik gösterir. Alıcının çözümlediği pseudorange değerleri ne kadar hatalıysa çözüm sonucu elde edilen konum da o ölçüde sapma içerir. Bu sapma özellikle

DOP (Dilution of Precision) değeri ile birlikte değerlendirildiğinde, GNSS performansının bir göstergesi haline gelir. Sinyal bozunumuna bağlı olarak:

- C/N_0 düştükçe çözüm kararsızlaşır,
- Pseudorange değerleri sapar,
- Uydu-alıcı mesafesinde milisaniyelik zaman farkları metrelerce hataya yol açar,
- Hatalı sinyallerin sayısı arttıkça RAIM (Receiver Autonomous Integrity Monitoring) sistemleri bile konumu güvenilir kılmakta zorlanır (Fu ve ark., 2025).

Özellikle spoofing saldırılarında, sinyalin kod fazı manipüle edilerek alıcıda yanıltıcı ama tutarlı bir konum üretilebilir. Bu, alıcının sinyali kaybetmesine neden olmadan sistematik konum sapmaları üretmesine yol açar ki bu durum savunma ve otonom navigasyon sistemleri için son derece tehlikelidir (Wang ve ark., 2017).

3.6. Jamming ve Spoofing'in Algılanması

GNSS sistemleri, zayıf sinyal yapıları nedeniyle çeşitli fiziksel ve elektromanyetik tehditlere karşı savunmasızdır. Bu tehditlerin başında gelen jamming ve spoofing saldırıları, konumlama ve zamanlama hizmetlerinin güvenilirliğini ciddi şekilde tehdit etmektedir. Bu nedenle GNSS alıcılarının bu tür saldırıları zamanında algılayabilmesi özellikle kritik uygulamalarda sistem bütünlüğünü korumak açısından hayati önem taşır (Wang ve ark., 2017).

Şekil 3.4. Jamming ve spoofing özet diyagramı

(Zhang ve ark., 2019)

3.6.1. Sinyal seviyesi tabanlı algılama yöntemleri

En yaygın kullanılan algılama yöntemleri, GNSS alıcısının doğrudan izleyebildiği fiziksel sinyal parametrelerine dayanır. Bu parametrelerdeki olağandışı değişimler, potansiyel bir saldırının işareti olabilir.

- **C/N₀ (Carrier-to-noise density ratio) anomalileri:** Sinyal-gürültü oranı GNSS alıcılarında sürekli izlenir. Jamming saldırıları sırasında bu değer belirgin şekilde düşerken, spoofing sırasında sahte sinyaller genellikle yüksek C/N₀ değerine sahip olabilir. Özellikle ani artışlar veya düşüşler, olağandışı bir müdahaleyi gösterebilir (Han ve ark., 2016).
- **AGC (Automatic gain control) seviyesi:** AGC, alıcının sinyal seviyesini sabit tutmak için kullandığı kazanç kontrol mekanizmasıdır. Ortamda ani güç artışı (örneğin jammer'ın devreye girmesi) durumunda AGC seviyesi değişir. Bu değişimler zaman içinde analiz edilerek saldırı tespiti yapılabilir (Akos, 2012).
- **SNR, Doppler, Faz kayması:** Spoofing saldırıları sırasında sinyalin Doppler frekansında veya taşıyıcı fazında tutarsızlıklar görülebilir. Bu değerlerin zamansal eğilimleri izlenerek sahte sinyallerle gerçek sinyaller arasındaki farklar ortaya çıkarılabilir (Egea-Roca ve ark., 2022).

3.6.2. Alıcı verisi ve tutarlılık tabanlı algılama

Alıcı içindeki konum çözümlemesi ve veri akışı incelenerek, GNSS sinyallerindeki tutarsızlıklar tespit edilebilir.

- **Pseudorange tutarsızlığı:** Spoofing saldırılarında, sahte sinyaller zamanlama açısından gerçek sinyallerden sapma gösterir. Bu sapmalar, pseudorange düzeyinde ani değişimler olarak gözlemlenebilir (Burbank ve ark., 2024). Çoklu alıcılardan alınan verilerin karşılaştırılması, bu farkların ayırt edilmesinde yardımcı olur.
- **RAIM (Receiver autonomous ıntegrity monitoring):** RAIM algoritmaları, çoklu uydulardan gelen veriler arasındaki tutarlılığı kontrol ederek, alıcının çözümlediği konumun güvenilirliğini değerlendirir. Jamming veya spoofing etkisi altında bu tutarlılık bozulduğunda, alıcı potansiyel hata durumunu raporlayabilir (Khawaja ve ark., 2015).
- **Çoklu anten / DoA (Direction of arrival) analizi:** GNSS sinyalleri normalde gökyüzünün farklı yönlerinden gelir. Ancak spoofing sırasında tüm sinyaller aynı

doğrultudan gelebilir. Çoklu antenli sistemlerde sinyal geliş yönü analiz edilerek bu anomali tespit edilebilir (Magiera ve Katulski, 2015).

3.6.3. Yapay zekâ ve makine öğrenmesi tabanlı algılama

Gelişen hesaplama teknolojileriyle birlikte makine öğrenmesi (Machine Learning) tabanlı yaklaşımlar da GNSS saldırılarını tespit etmede etkili hale gelmiştir. Bu yöntemlerde, alıcılardan toplanan çeşitli parametreler (C/N_0 eğrileri, AGC değerleri, konum sapmaları vb.) sınıflandırma algoritmalarına giriş verisi olarak kullanılır.

SVM (Support Vector Machines) ile sahte sinyal örüntüleri yüksek doğrulukla ayrıştırılabilir. Karar ağaçları ve k-en yakın komşu (k-NN) algoritmaları, saldırı tipi sınıflamasında başarılı sonuçlar vermektedir (Schmidt ve ark., 2016). Derin öğrenme temelli yapay sinir ağları, büyük veri setlerinden özellik çıkartarak saldırı tespiti gerçekleştirebilir.

Bu yöntemlerin başarımı; kullanılan veri kümesinin büyüklüğü, saldırı tipi ve sistem mimarisi gibi değişkenlere bağlıdır. Gerçek zamanlı saldırı tespit sistemlerinde düşük gecikmeli modeller tercih edilir.

4. MATERYAL VE YÖNTEM

4.1 Adalm Pluto Cihazı Yapısı ve Teknik Özellikleri

Bu tez çalışmasında Adalm Pluto cihazı, GNSS spoofing saldırılarının gerçekleştirilmesi amacıyla kullanılmıştır. Cihaz, GPS sinyallerini taklit eden sahte sinyallerin oluşturulmasında bir sinyal yayıcı (transmitter) olarak işlev görmüştür. Özel olarak yapılandırılmış yazılım tanımlı sinyaller, PlutoSDR aracılığıyla GNSS alıcısına iletilmiş; böylece alıcının gerçek sinyaller yerine bu sahte sinyallere kilitlenmesi sağlanarak yanıltıcı konum üretimi gerçekleştirilmiştir.

PlutoSDR'nin küçük yapısı ve programlanabilirliği sayesinde farklı sinyal iletimi test edilmiştir. Deneysel süreçte cihaz, dış ortam senaryolarında test edilerek sinyal gücü, etki menzili ve yanıltma başarısı analiz edilmiştir. Bu bağlamda PlutoSDR, spoofing saldırılarının kontrollü biçimde uygulanmasına olanak sağlayarak GNSS sistemlerinin zafiyetlerinin gözlemlenmesinde kilit rol oynamıştır.

ADALM-PLUTO (PlutoSDR), Analog Devices firması tarafından eğitim ve araştırma amaçlı geliştirilmiş, yazılım tanımlı radyo (SDR – Software Defined Radio) mimarisine sahip kompakt bir RF donanımıdır. ADALM, "Active Learning Module" (Etkin Öğrenme Modülü) ifadesinin kısaltmasıdır ve cihaz, sinyal işleme ve kablosuz haberleşme sistemleri üzerine gerçek zamanlı deneyler yapılabilmesi için tasarlanmıştır (Analog Devices, 2020).

PlutoSDR, AD9363 RF transceiver çipi ve Xilinx Zynq Z7010 SoC mimarisiyle çalışmakta olup, hem iletim (transmit, TX) hem de alım (receive, RX) yapabilme özelliğine sahiptir. Cihazın temel teknik özellikleri aşağıdaki gibidir:

- Frekans aralığı: 325 MHz – 3.8 GHz (bazı firmware güncellemeleriyle 70 MHz – 6 GHz'e çıkarılabilir).
- Bant genişliği: 20 MHz'e kadar anlık spektrum işleyebilir.
- Çift kanal (1 TX / 1 RX).
- USB 2.0 arabirimi ile bilgisayara bağlanır.
- GNU Radio, MATLAB/Simulink, SDR# gibi yazılımlarla uyumludur.

Kompakt yapısı, düşük maliyeti ve açık kaynak yazılım desteği sayesinde PlutoSDR, özellikle GNSS araştırmaları, spektrum analizleri, jamming/spoofing testleri ve haberleşme prototipleme uygulamalarında sıklıkla tercih edilmektedir (Schmidt ve ark., 2018).

Şekil 4.1. Adalm pluto cihazı

4.2. HackRF One Cihazı Yapısı ve Teknik Özellikleri

Bu tez kapsamında HackRF One cihazı, GNSS sinyallerine yönelik jamming saldırılarının gerçekleştirilmesi amacıyla kullanılmıştır. Özellikle beyaz gürültü (white noise) ve dar bant parazit sinyalleri oluşturularak, GPS alıcısının taşıyıcı sinyali çözümleyememesi ve konum bilgisi üretiminde başarısız olması hedeflenmiştir.

HackRF One cihazı, özel olarak hazırlanmış GNU Radio tabanlı sinyal akış diyagramları aracılığıyla sinyal üreticisi olarak konumlandırılmış; belirli mesafelerden gerçekleştirilen deneylerde GNSS alıcısının performansı analiz edilmiştir. Bu süreçte cihaz, farklı frekans genişliklerinde ve çıkış güçlerinde test edilmiş; taşıyıcı-gürültü oranı (C/N_0) üzerindeki etkisi gözlemlenmiştir. Tez çalışmasında, HackRF One'ın GNSS karıştırma saldırılarının etkili ve kontrollü bir biçimde gerçekleştirilmesine olanak sağlayan temel SDR cihazı olduğu sonucuna ulaşılmıştır.

HackRF One, Great Scott Gadgets firması tarafından geliştirilen, açık kaynaklı ve çok amaçlı bir SDR donanımıdır. 1 MHz ile 6 GHz arasında geniş bir frekans aralığında çalışabilen HackRF One, özellikle kablosuz haberleşme, sinyal analizleri, protokol çözümleme ve güvenlik testleri gibi uygulamalarda yaygın olarak tercih edilmektedir (Janos ve Kuras, 2021).

Bu cihaz, yarı çift yönlü (half-duplex) çalışma prensibine sahiptir; yani aynı anda hem alım (RX) hem de iletim (TX) işlemi yapamaz. Ancak hızlı geçiş yaparak sinyal üretimi ve analizi için yeterli esnekliği sağlar. Entegre RF ön uç devreleri sayesinde çeşitli modülasyon türlerini destekler ve GNU Radio, SDR#, GQRX gibi popüler açık kaynak SDR yazılımlarıyla tam uyumlu çalışır.

Temel teknik özellikleri:

- Frekans aralığı: 1 MHz – 6 GHz
- Örnekleme hızı: 20 Msps
- Çözünürlük: 8 bit ADC
- Bağlantı: USB 2.0
- Maksimum çıkış gücü: ~10 dBm (cihaza ve frekansa bağlı olarak değişken)

HackRF One, düşük maliyetli olması, açık kaynak donanım-yazılım yapısı ve taşınabilirliği ile güvenlik araştırmacıları ve akademisyenler arasında popülerlik kazanmıştır. GNSS güvenlik çalışmaları özelinde, jamming ve spoofing saldırılarının simülasyonunda sıklıkla kullanılan SDR cihazlarından biridir (Janos ve Kuras, 2021).

Şekil 4.2. HackRF One cihazı

4.3. LoRa Anten Yapısı ve Teknik Özellikleri

Bu tez çalışmasında LoRa anten, özellikle açık alan deneylerinde HackRF One cihazı ile birlikte kullanılmış ve jamming sinyallerinin daha geniş alana yayılarak GNSS alıcısı üzerindeki etkisinin mesafe bazlı gözlemlenmesi sağlanmıştır. Düşük frekanslı parazit sinyallerin yayılmasında tercih edilmesi, çevresel engellerin daha kolay aşılmasını sağlamış; bu sayede 15 metre ve 25 metre mesafelerde yapılan testlerde daha etkin jamming etkisi elde edilmiştir.

LoRa (Long Range) anten, düşük güçlü, uzun menzilli kablosuz iletişim sistemlerinde kullanılan ve özellikle 433 MHz, 868 MHz veya 915 MHz gibi frekanslarda çalışan yönsüz veya yarı yönlü RF antenleridir. Genellikle IoT (Nesnelerin İnterneti) uygulamalarında tercih edilen bu antenler, düşük frekanslı GNSS bozucu sinyallerin yayılımında da etkili bir role sahiptir (Augustin ve ark., 2016).

Teknik Özellikleri:

- Çalışma frekansı: 868 MHz (bu çalışmada kullanılan model)
- Kazanç: 2–5 dBi arası
- Yönsüz yayın (omnidirectional)
- VSWR: ≤ 2.0 (çıkış uyumu)
- Bağlantı türü: SMA erkek

Şekil 4.3. LoRa anten

4.4 2.4 GHZ Anten Yapısı ve Teknik Özellikleri

Bu tez çalışmasında 2.4 GHz anten, özellikle PlutoSDR cihazıyla birlikte sahte GNSS sinyallerinin iletiminde kullanılmıştır. Deneylerin kısa mesafe (~5 m) spoofing testlerinde bu antenin kullanımı, sinyalin kararlı ve güçlü biçimde iletilmesini sağlamış; alıcının sinyal kaynağını tanımadan sahte sinyale kilitlenmesi başarılmıştır. Ayrıca antenin kısa dalga boyu, çoklu yol (multipath) etkisini artırmadan net bir sinyal yayımı sunmuştur.

2.4 GHz bandında çalışan RF antenleri, Wi-Fi, Bluetooth, Zigbee ve çeşitli kablosuz veri aktarım sistemlerinde yaygın olarak kullanılmaktadır. Bu antenler, daha yüksek frekanslı sinyallerin iletimi ve hedefli uygulamalarda tercih edilmektedir. GNSS spoofing uygulamalarında ise özellikle sahte sinyallerin belirli yönlere yönlendirilmesi ve kısa menzilli deneylerde sinyal netliğinin artırılması amacıyla kullanılmıştır (Dovis, F. (Ed.). (2015).

Teknik Özellikleri:

- Çalışma frekansı: 2.4–2.5 GHz
- Kazanç: 3–9 dBi (kullanılan modele göre)
- Yönlülük: Yönsüz veya yarı yönlü (dipol / panel)
- Bağlantı tipi: RP-SMA / SMA

Şekil 4.4. 2.4 GHZ anten

4.5. Trimble GNSS Alıcısı Yapısı ve Teknik Özellikleri

Bu tez çalışmasında Trimble GNSS alıcısı, jamming ve spoofing saldırılarının GNSS konum doğruluğu üzerindeki etkilerini analiz etmek amacıyla referans alıcı olarak kullanılmıştır. Trimble'ın yüksek hassasiyetli konumlama kapasitesi sayesinde, normal çalışma koşullarındaki konum verileri ile saldırı altındaki koşullarda alınan veriler karşılaştırılmış ve mutlak konum sapmaları, C/N_0 düşüşleri ve uydu kilitlenme problemleri gibi performans bozulmaları istatistiksel olarak değerlendirilmiştir.

Trimble alıcısı, deneysel kurgu kapsamında dış mekânda gerçekleştirilmiş olan jamming ve spoofing senaryoları sırasında aktif olarak konum ölçümü yapmış; belirli mesafelerden uygulanan saldırılar karşısında alıcının verdiği tepkiler kaydedilmiştir. Böylece cihaz, saldırı etkilerinin nicel olarak ortaya konulmasında karşılaştırmalı veri kaynağı olarak görev yapmıştır (Leick ve ark., 2015).

Ayrıca Trimble'ın C/N_0 değerlerini anlık olarak kaydedebilme, uydu görünürlüğünü izleyebilme ve konum çözüm modlarını (RTK, float, stand-alone) analiz edebilme yetenekleri sayesinde, alıcının saldırılara verdiği teknik tepkiler detaylı olarak değerlendirilmiş ve GNSS güvenliği açısından zayıf noktalar tespit edilmiştir.

Trimble GNSS alıcıları, hassas konum belirleme gerektiren mühendislik, haritacılık, inşaat ve jeodezi gibi disiplinlerde yaygın olarak kullanılan yüksek doğruluklu uydu alıcı sistemleridir. Trimble, GNSS teknolojisinde öncü firmalardan biri olup, sunduğu alıcılar; GPS, GLONASS, Galileo ve BeiDou gibi birden fazla uydu sistemini destekleyerek küresel düzeyde güvenilir ve kesintisiz konum bilgisi sağlamaktadır (Trimble Inc., 2021).

Kullanılan modele bağlı olarak Trimble alıcılar, RTK (Real-Time Kinematic) ve PPP (Precise Point Positioning) gibi hassas konumlama yöntemlerini desteklemekte; taşıyıcı faz izleme, çoklu frekans kullanımı ve parazit bastırma algoritmaları ile donatılmıştır. Trimble GNSS alıcıları; sağlam gövde yapısı, uzun pil ömrü, çevresel dayanıklılığı ve yüksek hassasiyetli anten yapısı ile öne çıkar (Misra, P., ve Enge, P. (2011).

Temel Teknik Özellikleri :

- Desteklenen sistemler: GPS, GLONASS, Galileo, BeiDou
- Çift veya üçlü frekans desteği: L1, L2, L5
- Konum doğruluğu: RTK ile 1–2 cm (yatay), 2–3 cm (düşey)
- Veri formatı: RINEX, RTCM, CMR
- Kullanıcı arayüzü: Entegre ekran veya harici kontrol ünitesi
- Kullanım türü: Statik, kinematik, gerçek zamanlı RTK

Şekil 4.5. Trimble GNSS Alıcısı

Şekil 4.6. Trimble GNSS alıcı ekipmanı

Şekil 4.7. Trimble GNSS alıcısı kontrol kumandası

4.6 Yazılım Tanımlı Radyo (SDR) Algoritması

Yazılım Tanımlı Radyo (Software Defined Radio – SDR), geleneksel donanımsal radyo bileşenlerinin (modülatör, demodülatör, filtre, frekans çevirici vb.) yazılım tabanlı olarak bir bilgisayar ya da gömülü sistem üzerinden tanımlanmasını ve kontrol edilmesini sağlayan bir teknolojidir. SDR sistemleri, donanımsal değişikliğe gerek kalmadan farklı iletişim protokollerinin, frekansların ve sinyal türlerinin esnek biçimde işlenmesini mümkün kılar (Mitola, 1995).

SDR mimarilerinde, RF sinyali bir analog–dijital çevirici (ADC) aracılığıyla sayısal ortama aktarılır ve sinyalin modülasyonu, frekans kaydırması, filtrelenmesi gibi işlemler tamamen yazılımsal olarak gerçekleştirilir. Bu yapı sayesinde kullanıcı, birden fazla kablosuz sistem arasında hızlı geçiş yapabilir, özel sinyaller oluşturabilir ve mevcut protokolleri değiştirebilir. (GNU Radio Foundation, (2023).

SDR algoritmaları genellikle aşağıdaki temel işlevleri içerir:

- Dalga şekli üretimi (waveform generation)
- Modülasyon / demodülasyon işlemleri
- Spektrum analizi ve sinyal taraması
- Gürültü üretimi veya bastırma
- Sinyal protokolü tanıma ve taklit etme

Bu tez çalışmasında SDR algoritmaları, GNSS sistemlerine yönelik jamming ve spoofing saldırılarının gerçekleştirilmesinde temel işlevsel katman olarak kullanılmıştır. HackRF One ve PlutoSDR cihazlarının sinyal üretici yetenekleri, doğrudan SDR algoritmaları ile yönlendirilmiş; sinyalin içeriği, gücü, frekansı ve zamanlaması yazılım üzerinden tanımlanarak saldırı senaryoları oluşturulmuştur.

4.7. Statik Ölçüm Metodu

Statik GNSS ölçüm yöntemi, bir GNSS alıcısının belirli bir noktada sabit bir süre boyunca konum verisi toplaması esasına dayanan, yüksek doğruluk gerektiren uygulamalarda tercih edilen bir konum belirleme metodudur. Bu yöntemde alıcı, belirlenen sabit noktaya yerleştirilir ve genellikle 20 dakika ila birkaç saat arasında değişen süre boyunca veri kaydı gerçekleştirir (Hofmann-Wellenhof ve ark., 2008).

Statik ölçüm, özellikle jeodezik ağların oluşturulması, zemin deformasyon analizleri, altyapı projeleri ve GNSS doğruluk analizleri gibi uygulamalarda kullanılır. Yüksek doğruluk elde edilmesini sağlayan temel faktör, uzun süreli veri toplama sayesinde atmosferik hataların ortalamasının alınabilmesi ve faz ölçümlerine dayalı konum düzeltmelerinin yapılabilmesidir.

Statik yöntemin temel özellikleri:

- Alıcı sabit kalır, ölçüm süresi uzundur.
- Taşıyıcı faz gözlemleri kullanılır.

- Yüksek doğruluk (santimetre düzeyi) sağlanabilir.
- Genellikle referans istasyon verisiyle birlikte değerlendirilir.

Bu tez çalışmasında statik ölçüm metodu, GNSS alıcısının jamming ve spoofing saldırıları altındaki davranışını karşılaştırmak için kullanılmıştır. Saldırı öncesi, sırası ve sonrasında alınan statik ölçümler ile konum kayması, sinyal kalitesi düşüşü ve çözüm tipi değişimleri analiz edilmiştir.

4.8. Kinematik Ölçüm Metodu

Kinematik GNSS ölçüm yöntemi, alıcının hareket hâlinde olduğu durumlarda gerçek zamanlı ya da post-processing yöntemiyle yüksek doğruluklu konum verisi üretmesini sağlayan bir ölçüm tekniğidir. Alıcının konumu sabit değil sürekli değişmektedir; bu nedenle konum çözüm algoritmaları, zamanla değişen uydu geometrisini ve faz farklarını dinamik olarak işlemelidir (Leick ve ark., 2015).

Kinematik yöntem, özellikle mobil haritalama, araç takip sistemleri, otomatik tarım, hidrografik ölçümler ve taşınabilir sensör ağları gibi alanlarda yaygın olarak kullanılmaktadır. Taşıyıcı faz ölçümleri ile entegre edilen RTK ya da PPP yöntemleri kullanıldığında, santimetre düzeyinde konum doğruluğu elde edilebilir.

Kinematik yöntemin temel özellikleri:

- Alıcı hareket hâlindedir.
- Gerçek zamanlı veya sonradan işleme ile analiz yapılabilir.
- Düşük gecikmeli ve yüksek frekanslı veri üretir.
- Uydu kilitlenme sürekliliği önemlidir.

Bu tez çalışmasında kinematik ölçüm yöntemi, GNSS alıcısının hareketli hâlde iken jamming ve spoofing saldırılarına verdiği tepkiyi gözlemlemek amacıyla kullanılmıştır. Alıcı, sabit bir güzergâh boyunca hareket ettirilmiş; saldırı öncesi ve saldırı anında izlenen rotalar, hata eğrileri ve konum sapmaları analiz edilmiştir. Bu sayede, saldırının hareket hâlindeki GNSS sistemleri üzerindeki etkisi daha gerçekçi biçimde değerlendirilmiştir.

4.9. Deney Uygulama Çalışması

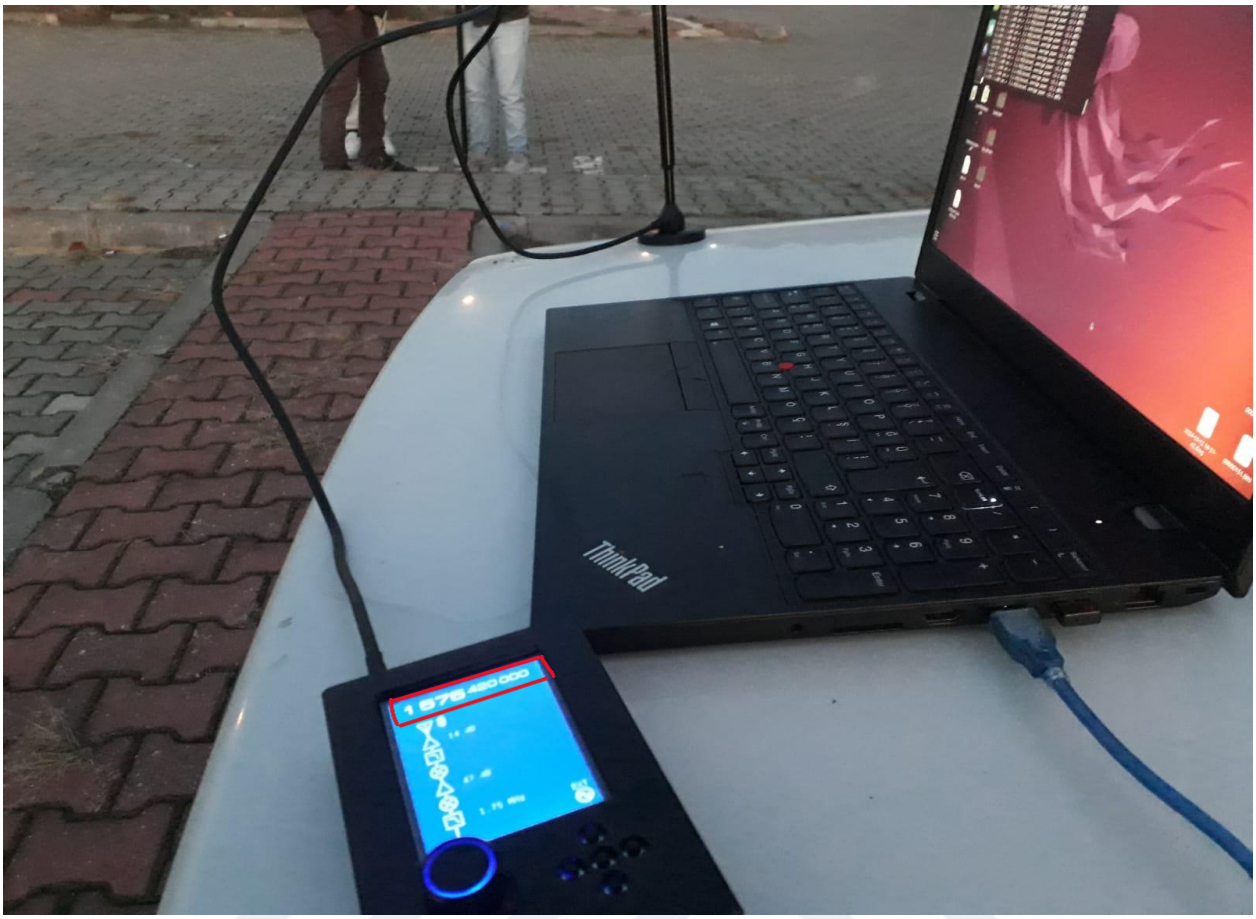
Bu tez kapsamında, GNSS sistemlerine yönelik jamming ve spoofing saldırılarının farklı mesafelerden uygulanarak alıcı üzerindeki etkilerinin incelenmesi amacıyla kontrollü bir deneysel kurgu oluşturulmuştur. Deneyler, hem statik (sabit konumda) hem de kinematik

(hareketli) ölçüm senaryoları için gerçekleştirilmiş; farklı anten türleri, frekanslar ve saldırı süreleri göz önünde bulundurulmuştur.

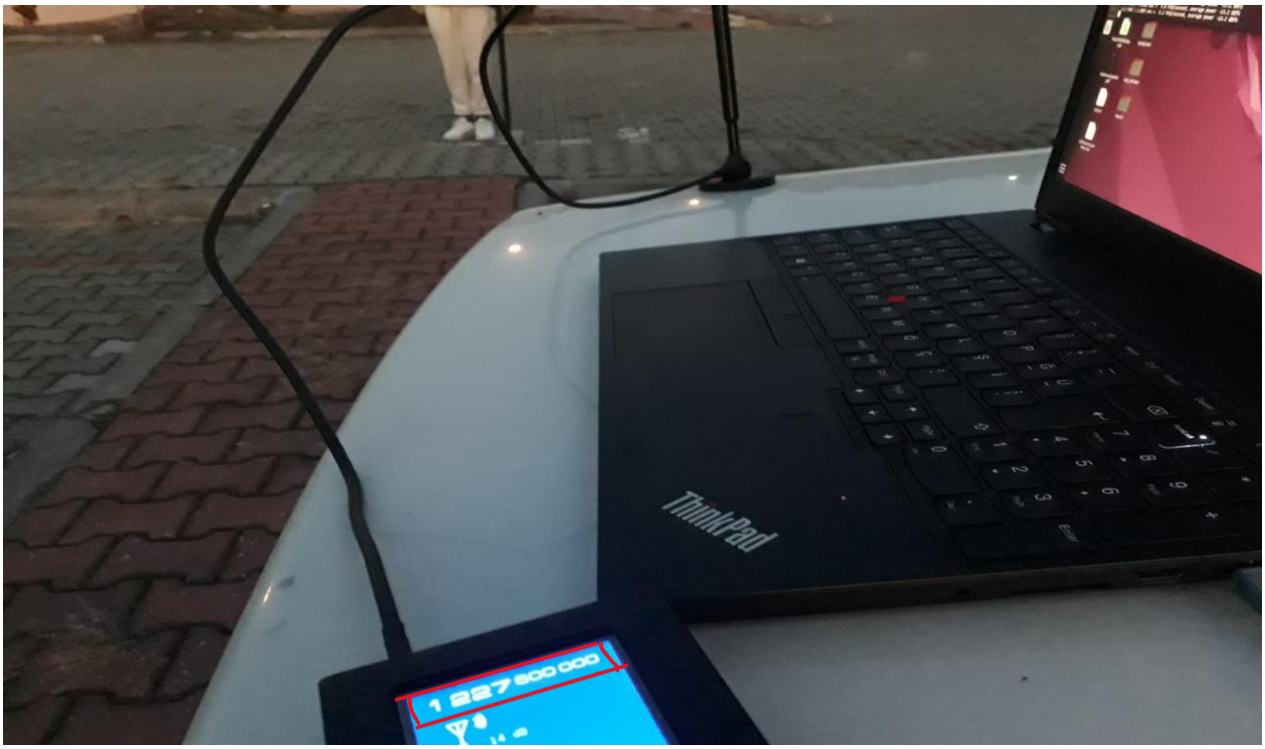
GNSS Jamming ve Spoofing Test Ölçüm Tablosu

Çizelge 4.1. Statik ve kinematik ölçüm

Anten No	Frekans	Senaryo	Zaman Aralığı
Anten 1	Lora	Serbest Ölçüm	12:00–12:30 (30 dakika)
Anten 1	Lora	Jamming (5 Metre)	12:30-12:35 (5 dakika)
Anten 1	Lora	Jamming (15 Metre)	12:35-12:40 (5 dakika)
Anten 1	Lora	Jamming (25 Metre)	12:40-12:45 (5 dakika)
Anten 2	2.4 GHz	Jamming (5 Metre)	12:45-12:50 (5 dakika)
Anten 2	2.4 GHz	Jamming (15 Metre)	12:50-12:55 (5 dakika)
Anten 2	2.4 GHz	Jamming (25 Metre)	12:55-13:00 (5 dakika)
Anten 1	Lora (L1 freq)	Spoofing (25 Metre)	13:00-13:05 (5 dakika)
Anten 1	Lora (L1 freq)	Spoofing (15 Metre)	13:05-13:10 (5 dakika)
Anten 1	Lora (L1 freq)	Spoofing (5 Metre)	13:10-13:15 (5 dakika)
Anten 1	Lora (L1 freq)	Spoofing (15 Metre)	13:15-13:20 (5 dakika
Anten 1	Lora (L2 freq)	Spoofing (5 Metre)	13:20–13:30 (10 dakika)



Şekil 4.8. GPS L1 frekansına(1575 MHz) jamming ve spoofing uygulama işlemi



Şekil 4.9. GPS L2 frekansına(1227 MHz) jamming ve spoofing uygulama işlemi

Şekil 4.10. 5 metre mesafeden uygulanan jamming ve spoofing uygulama işlemi

Şekil 4.11. 15 metre mesafeden uygulanan jamming ve spoofing uygulama işlemi

Şekil 4.12. 25 metre mesafeden uygulanan jamming ve spoofing uygulama işlemi

4.10. Ölçüm Protokolü ve Veri Analiz Yöntemi

Bu tez kapsamında gerçekleştirilen jamming ve spoofing deneyleri, hem sabit hem de hareketli (kinematik) konum senaryolarında GNSS alıcısının performansını nicel olarak değerlendirmeye yönelik olarak yapılandırılmıştır. Ölçüm protokolü, deneysel doğruluk ve tekrar edilebilirlik ilkeleri doğrultusunda planlanmış ve verilerin analizi için çok boyutlu değerlendirme yöntemleri uygulanmıştır.

4.10.1. Ölçüm protokolü

Bu çalışmada, GNSS alıcılarının jamming ve spoofing saldırılarına karşı duyarlılığını değerlendirmek amacıyla kontrollü bir ölçüm protokolü uygulanmıştır. Ölçümler, açık alanda GNSS sinyalinin doğrudan alınabildiği bir ortamda gerçekleştirilmiştir. Deneysel kurgu kapsamında, öncelikle referans niteliğinde serbest konum verileri toplanmış; ardından farklı mesafelerden (5 m, 15 m, 25 m) sırasıyla jamming ve spoofing sinyalleri uygulanmıştır. Uygulama süresince GNSS alıcısı, taşıyıcı faz ve kod çözüm verilerini toplarken; eş zamanlı olarak Adalm Pluto ve HackRF One cihazları yardımıyla saldırı sinyalleri gönderilmiştir. Her senaryoda sabit bir anten konfigürasyonu korunmuş ve farklı frekans bandında çalışan Lora ve 2.4 GHz antenler kullanılmıştır. Statik ve kinematik modlar ayrı ayrı değerlendirilmiş; her ölçüm periyodu sonunda konum sapmaları, çözüm kararlılığı ve hata oranları analiz edilmiştir.

4.10.2. Referans ölçümü

Deneysel sürecin başlangıcında GNSS alıcısı üzerinde hiçbir harici müdahale olmadan 30

dakikalık bir serbest ölçüm alınmıştır. Bu süreçte elde edilen konum verileri, sonraki saldırı senaryolarında referans (baz konum) olarak kullanılmıştır.

4.10.3. Jamming senaryoları

İki farklı anten (LoRa ve 2.4 GHz), her biri üç farklı mesafede (yaklaşık 5 m, 15 m ve 25 m) konumlandırılarak GNSS sinyaline jamming sinyalleri uygulanmıştır. Her uygulama yaklaşık 5 dakika süreyle gerçekleştirilmiş, saldırı süresince GNSS alıcısının konum çözüm kalitesi, uydulara ait C/N_0 değerleri ve uydu görünürlüğü izlenmiştir. Jamming sinyalleri SDR algoritmaları aracılığıyla oluşturulmuştur.

4.10.4. Spoofing senaryoları

PlutoSDR cihazı ile oluşturulan sahte GNSS sinyalleri, LoRa anteni aracılığıyla farklı frekanslarda (L1 ve L2) ve mesafelerde GNSS alıcısına yönlendirilmiştir. Spoofing sürecinde alıcının gerçek konumdan sapma davranışı, çözüm tipi, alıcı yeniden başlatma gereksinimi gibi parametreler gözlemlenmiş ve kayıt altına alınmıştır. Her spoofing uygulaması yaklaşık 8–10 dakika sürmüştür.

4.10.5. Kinematik ölçüm senaryoları

GNSS alıcısı sabit bir rota üzerinde hareket ettirilmiş ve hem saldırı altında hem de saldırısız (jamsiz) koşullarda ölçümler yapılmıştır. Kinematik ölçümde rotadan sapma, izlenen yolun uzunluğu, hata elipsleri gibi parametreler değerlendirilmiş; zamana bağlı konum bozulmaları analiz edilmiştir.

4.11 Veri Analiz Yöntemi

Toplanan GNSS verileri, Trimble alıcısının sunduğu ham veriler (RINEX, NMEA) ve ek olarak SDR cihazlarının zaman-dalga kayıtları üzerinden analiz edilmiştir. Aşağıdaki analiz yöntemleri kullanılmıştır:

4.11.1 C/N_0 (Carrier-to-noise density ratio) analizi

Sinyal kalitesini doğrudan etkileyen C/N_0 değeri, jamming senaryolarında belirgin düşüş göstermiştir. Saldırı öncesi ve sonrası C/N_0 değişimleri zaman serisi olarak grafiksel biçimde karşılaştırılmıştır.

4.11.2 Konum sapma hesaplaması

Saldırı sırasında elde edilen konumlar, referans konuma göre karşılaştırılmış; ortalama sapma maksimum hata, standart sapma gibi istatistiksel ölçütler hesaplanmıştır.

4.11.3 Çözüm tipi takibi

Her ölçümde GNSS alıcısının çözüm tipi (RTK Fixed, RTK Float, Single, No Fix) izlenmiş ve zaman içinde yaşanan geçişler zamana bağlı olarak grafikleştirilmiştir.

4.11.4 Kinematik analiz

Kinematik rota verileri Coğrafi Bilgi Sistemleri (CBS) ortamında analiz edilmiş; rotadan sapma mesafesi, yön değişim anomalileri ve spoofing altındaki tutarsızlıklar belirlenmiştir.

5. BULGULAR VE TARTIŞMA

5.1. Kinematik Ölçüm Sonuçları

Ölçümler, kinematik modda yapılmış olup, bu da GNSS alıcısının sabit değil, hareket hâlinde olduğu anlamına gelmektedir. Bu bağlamda, jamming ve spoofing saldırılarının kinematik konum belirleme üzerindeki etkilerinin analizine yönelik önemli bir veri kaynağıdır. Elde edilen veriler RİNEX formatına çevrilmiş olup Kanada merkezli CSRS-PPP GNSS firmasına veriler gönderilmiş ve işlenmiştir (https://webapp.csrs-scrs.nrcan-rncan.gc.ca/geod/tools-outils/ppp.php).

5.1.1 Kinematik PPP çözümünün genel özeti

CSRS-PPP 4.14.11 (2024-11-29)

93650030.25o
57

Data Start	Data End	Duration of Observations
2025-01-03 11:51:05.00	2025-01-03 13:34:19.99	1:43:14.990
Processing Time		**Product Type**
15:34:07 UTC 2025/01/03		NRCan Ultra-rapid
Observations	**Frequency**	**Mode**
Phase and Code	Double	Kinematic

Elevation Cut-Off	Rejected Epochs	Fixed Ambiguities	Estimation Steps
7.5 degrees	4.34 %	44.93 %	5.00 sec

Antenna Model	APC to ARP	ARP to Marker
TRM60158.00 NONE	L1 = 0.085 m L2 = 0.081 m	H:1.465m / E:0.000m / N:0.000m

(APC = antenna phase center; ARP = antenna reference point)

Estimated ITRF Positions for 93650030.25o can be found in 93650030.pos

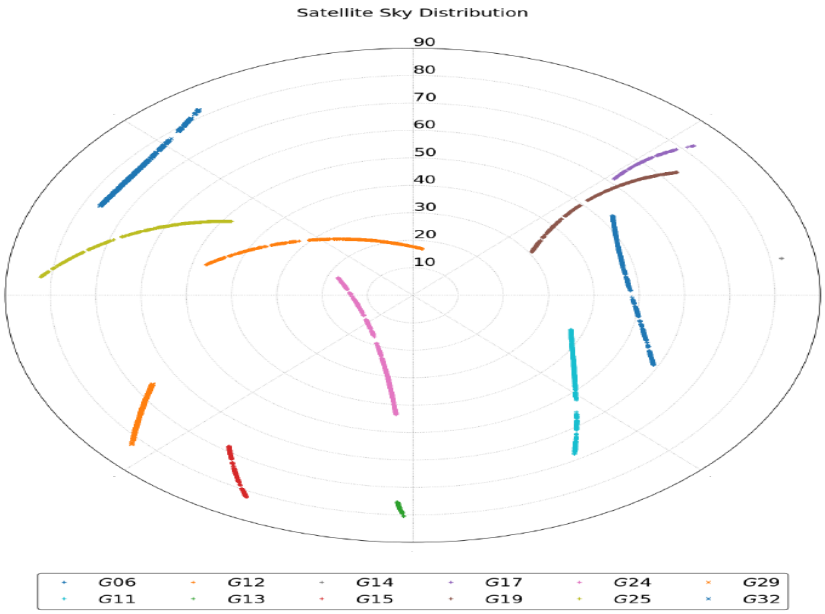
Şekil 5.1. Kinematik PPP çözümünün genel özeti

5.1.2. Kinematik ölçüm ve işlem parametrelerinin değerlendirilmesi

Çizelge 5.1. Ölçüm ve işlem parametrelerinin değerlendirilmesi

Parametre	**Açıklama**
Mode	*Kinematic*: Alıcının hareket halinde olduğunu dinamik bir ölçüm olduğunu gösterir.
Frequency	*Double*: L1 ve L2 olmak üzere çift frekans kullanılmıştır.
Observations	*Phase and Code*: Hem kod hem de taşıyıcı faz verisi kullanılmıştır.
Elevation Cut-Off	7.5°'den daha küçük açılarla gelen uydular çözüme dahil edilmemiştir.
Rejected Epochs	*%4.34*: Gözlemlerin %4.34'ü reddedilmiş. Bu oran düşük kabul edilir ve verinin genel kalitesinin iyi olduğunu gösterir.
Fixed Ambiguities	*%44.93*: Taşıyıcı faz çözümlemesinde belirsizliklerin yaklaşık %45'i sabitlenebilmiştir. Bu oran, jamming/spoofing etkisinin varlığına işaret etmektedir; zira ideal koşullarda bu oranın%80 civarında olması beklenir.
Estimation Steps	*5.00 sec*: Her 5 saniyede bir pozisyon çözümü yapılmıştır.
Antenna Model	*TRM60158.00 NONE*: Trimble marka, çift frekans destekli hassas GNSS anteni kullanılmıştır.
APC to ARP	L1 = 0.085 m, L2 = 0.081 m: Antenin faz merkezi ile referans noktası arasındaki yükseklik farklarıdır.
ARP to Marker	H:1.465 m: Anten yüksekliği olarak hesaplamaya dahil edilmiştir.

5.1.3. Kinematik uydu gökyüzü dağılımı (Sky plot) analizi



Şekil 5.2. Kinematik uydu gökyüzü dağılımı analizi

Yukarıda gösterilen uydu gökyüzü dağılım grafiği, ölçüm süresince GNSS alıcısı tarafından izlenen uyduların yatay açı ve yükselti değerlerini temsil etmektedir. Bu grafik, sinyal kalitesinin yorumlanması ve parazit kaynaklarına karşı uydu görünürlüğünün incelenmesi açısından önemlidir.

Grafikte yer alan uydu tanımlayıcılarına (örn. G06, G11, G24) bakıldığında, ABD'ye ait GPS uydularının (Gxx kodları) kullanıldığı anlaşılmaktadır. En az 12 farklı GPS uydusunun izlendiği görülmektedir. Bu sayede GNSS alıcısı hem yatay hem de düşey konumlamada yeterli uydu çözümlemesi yapabilmiştir. Her bir uyduya ait renkli eğriler, o uydunun ölçüm süresi boyunca alıcı tarafından ne kadar süreyle takip edilebildiğini gösterir. Bazı uydular daha kısa süreyle (örneğin G14, G15), bazıları ise daha uzun süreyle izlenmiştir (örneğin G06, G11, G32). Bu farklılıklar, anten görüş alanı, çevresel engeller veya jamming etkileriyle ilişkili olduğunu göstermektedir.

Uydu dağılımının dengeli olmasına rağmen belirsizliklerin sadece %44.93'ünün sabitlenebilmiş olması, jamming/spoofing uygulamaları sırasında bazı uyduların geçici olarak sinyal kaybına uğradığını ya da C/N_0 seviyesinin düştüğünü göstermektedir. Özellikle düşük yükseklik açısındaki uyduların bu saldırılardan daha çok etkilendiği bilinmektedir.

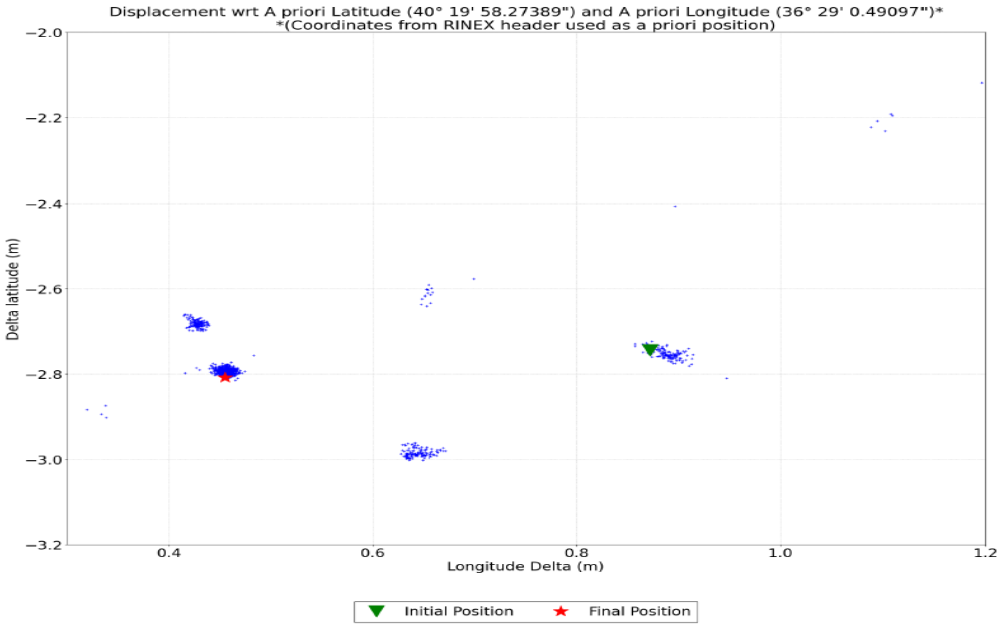
Gökyüzü dağılım grafiği, GNSS alıcısının ölçüm süresince çeşitli GPS uydularını farklı açılardan güvenilir biçimde izlediğini göstermektedir. Ancak taşıyıcı faz sabitleme oranının

düşüklüğü ve bazı uyduların sınırlı süreyle izlenmesi, jamming ve spoofing etkilerinin özellikle düşük açıyla gelen sinyaller üzerinde belirgin hale geldiğine işaret etmektedir.

Bu grafik, sinyal bozunumu altında dahi sistemin temel işlevlerini sürdürebildiğini; ancak doğruluk ve süreklilik açısından belirgin sapmaların yaşanabileceğini ortaya koymaktadır.

5.1.4. Kinematik konum sapması dağılımı analizi

Grafikte, GNSS ölçümleri süresince elde edilen tüm konum çözümleri, RINEX başlığında belirtilen referans koordinatlara göre hesaplanan delta (fark) değerleri ile gösterilmiştir. Bu farklar, boylam (Longitude Delta) ve enlem (Latitude Delta) eksenlerinde metre cinsinden sunulmuştur.



.

Şekil 5.3. Kinematik konum sapması dağılımı analizi

Grafik Bileşenleri:

Mavi noktalar: Tüm ölçüm süresi boyunca kaydedilen konum noktalarıdır.

Yeşil üçgen : Ölçümlerin başlangıcında elde edilen ilk konum çözümüdür.

Kırmızı yıldız : Son konum çözümüdür.

Ölçümler birkaç farklı kümeye dağılmış durumdadır. Bu, alıcının belirli zaman aralıklarında konum çözümünü farklı konumlar üzerinde sabitlediğini göstermektedir. Kümelerin yatay eksendeki (Longitude Delta) dağılımı yaklaşık 0.4 m ile 1.0 m aralığındadır. Dikey eksendeki (Latitude Delta) fark ise -2.6 m ile -3.0 m arasında değişmektedir. Bu, GNSS alıcısının saldırı

öncesi ve sonrası konum çözümünün belirgin şekilde değiştiğini, yani sinyal güvenilirliğinin bozulduğunu göstermektedir. Konum çözüm kümeleri oldukça sıkı olsa yani kendi içinde kararlı olsa da farklı kümeler arası sapmalar saldırı etkisinin büyüklüğünü ortaya koymaktadır.

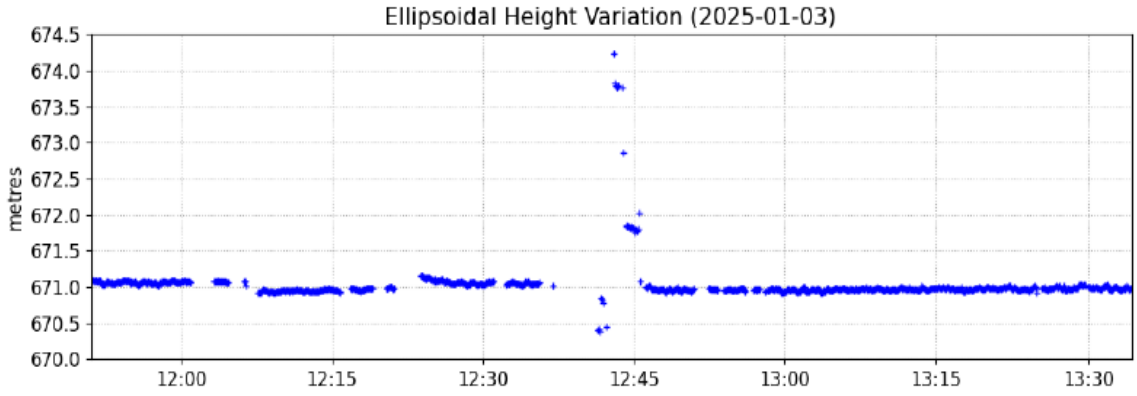
Konum çözüm kümelerinin birbirinden ayrık olması, özellikle spoofing saldırılarında beklenen tipik davranıştır**.** GNSS alıcısı, sahte sinyalleri gerçek sanarak konumunu farklı koordinatlara sabitlemiştir.

Jamming saldırıları sırasında alıcı, sinyal kalitesinin düşmesiyle farklı konumlara sıçrama veya çözümde belirsizlik yaşayabilir. Bu durum, kümeler arası konum sıçramalarını açıklamaktadır.

Konum Kararlılığı yüksek, ancak doğruluk düşüktür. Her kümenin içinde konumlar tutarlıdır ancak gerçek konumdan mutlak anlamda sapma mevcuttur. Bu da GNSS alıcısının yanlış pozisyonu sabit şekilde kabul ettiğini gösterir.

Bu dağılım grafiği, jamming ve özellikle spoofing saldırılarının GNSS alıcısı üzerinde oluşturduğu etkileri doğrudan göstermektedir. Konum çözümünde yaşanan sıçramalar, sistemin güvenilirliğinin azaldığını ve konum doğruluğunun bozulduğunu ortaya koymaktadır. Her ne kadar alıcı kendi içinde kararlı çözüm üretmiş olsa da, sahte sinyallere yönelerek gerçek konumdan sapması, bu tür saldırıların etkisini sayısal olarak doğrulamaktadır.

5.1.5. Kinematik elipsoidal yükseklik zaman serisi analizi



Şekil 5.4. Kinematik elipsoidal yükseklik zaman serisi analizi

Ölçüm başlangıcından yaklaşık 12:42'ye kadar (GPS saati ile gerçek saat farklılık gösterebilir.) yükseklik değerleri 670.8 – 671.1 m aralığında sabit kalmıştır. Bu, GNSS çözümünün istikrarlı olduğunu, uydu görünürlüğünün yeterli ve sinyal kalitesinin iyi olduğunu gösterir.

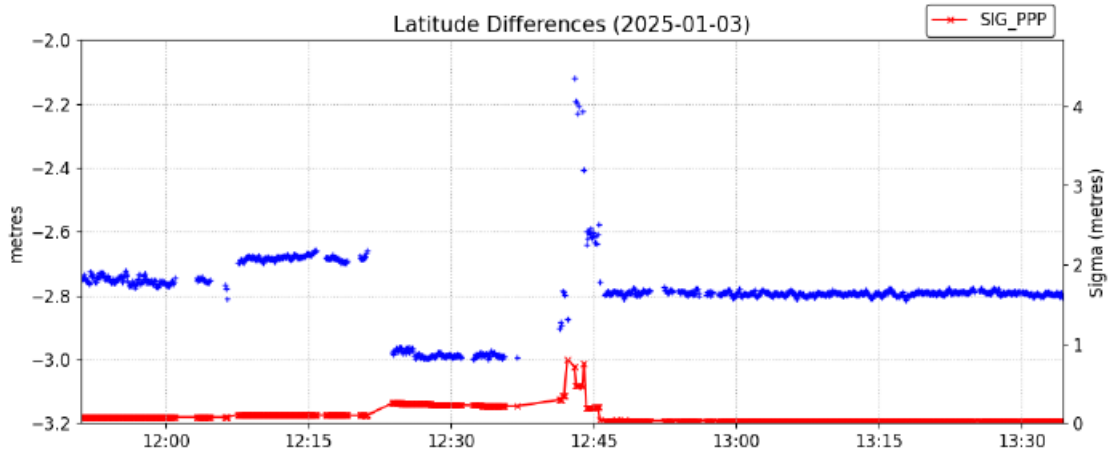
12:42 – 12:46 aralığında belirgin bir yükseklik sapması meydana gelmiştir. Bu sapma yaklaşık 3 metreye kadar yükselmiş ve 674.3 m civarına ulaşmıştır. Bu sıçrama, GNSS çözümünün geçici olarak bozulduğunu ve sistemin yanlış yükseklik üretmeye başladığını gösterir.

Bozulma süresi yaklaşık 4 dakika sürmüş ve sonrasında yükseklik değerleri tekrar önceki düzeye (671 m) dönmüştür. Bu, sinyal müdahalesi jamming veya spoofing gibi geçici bir etkene işaret etmektedir.

Müdahalenin sona ermesiyle birlikte alıcı, yeniden sabit ve güvenilir yükseklik çözümü üretmeye başlamıştır. Bu toparlanma, sistemin kendi içinde otomatik hata telafi mekanizmasına sahip olduğunu gösterir.

Bu grafik, GNSS sinyallerine yönelik saldırıların yalnızca yatay konum doğruluğunu değil, aynı zamanda elipsoidal yükseklik çözümünü de ciddi biçimde etkileyebildiğini açıkça göstermektedir. Özellikle kritik uygulamalarda (ör. insansız hava aracı uçuşları, hassas mühendislik ölçümleri), bu tür dikey sapmalar güvenlik risklerini beraberinde getirebilir.

5.1.6. Kinematik enlem farkı ve sigma (Çözüm belirsizliği) zaman serisi analizi



Şekil 5.5. Kinematik enlem farkı ve sigma zaman serisi analizi

Bu grafikte GNSS ölçüm elde edilen konumların enlem bileşenindeki sapmalarını (mavi çizgi) ve bu sapmalara karşılık gelen çözüm belirsizliklerini (kırmızı çizgi – SIG_PPP) zaman serisi olarak göstermektedir. Eksenler şu şekilde yapılandırılmıştır:

- Yatay eksen: Zaman
- Sol dikey eksen (mavi): Enlem farkı (metre cinsinden)

- Sağ dikey eksen (kırmızı): Sigma değeri, yani çözüm güven aralığı (metre cinsinden)

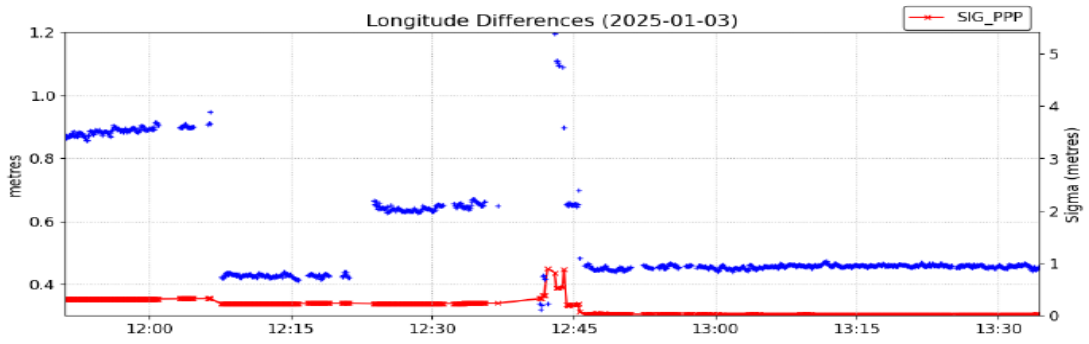
12:00 – 12:42 arası enlem farkları genellikle -2.6 m ile -3.0 m arasında sabit kalmıştır. Bu dönem boyunca SIG_PPP değeri ise 0.1 m ile 0.3 m aralığındadır. Bu durum, sistemin yüksek güvenilirlikte ve stabil konum çözümü ürettiğini gösterir.

12:42 – 12:46 arası hem enlem farkı hem de SIG_PPP değerleri belirgin şekilde artış göstermektedir. Enlem farkı yaklaşık -2.2 m'ye kadar yükselmiş, SIG_PPP değeri ise 3.5 metreyi aşmıştır. Bu ani sapma, GNSS çözümünün güvenilirliğinin ciddi oranda düştüğünü, sinyal bozunumuna veya sinyal aldatmaya maruz kalındığını kuvvetle göstermektedir.

12:46 sonrası hem konum farkı hem de sigma değeri tekrar düşmektedir. Bu da sistemin kendini toparladığını, yeniden güvenilir çözüm moduna geçtiğini gösterir.

Bu grafik, GNSS çözümünün sadece konumsal sapmalarla değil, aynı zamanda istatistiksel belirsizlikle de izlenebileceğini net şekilde ortaya koymaktadır. 12:42–12:46 arası yaşanan ani bozulma, jamming ya da spoofing etkisi altında GNSS sisteminin ne derece kararsız ve güvensiz hâle geldiğini ortaya koyar. Bu tür grafikler, sadece konum doğruluğunu değil, veri güvenilirliğini ölçmek açısından da kritik öneme sahiptir.

5.1.7. Kinematik boylam farkı ve çözüm belirsizliği zaman serisi



Şekil 5.6. Kinematik boylam farkı ve çözüm belirsizliği zaman serisi

Bu grafik, GNSS sisteminden elde edilen konumların referans boylam koordinatına göre gösterdiği farkları (mavi) ve çözümün güvenilirliğini (sigma – kırmızı) zaman ekseninde sunmaktadır.

Saat 12:00 – 12:42 arası boylam farkı yaklaşık 0.35 – 0.85 metre arasında dalgalanmakta, bu da doğal sebepler ve uydu dizilimi gibi faktörlerden kaynaklanan küçük oynamaları

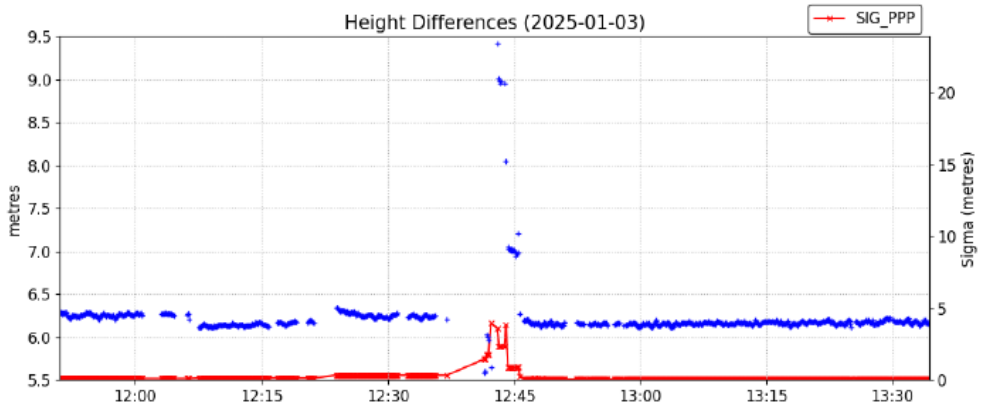
göstermektedir.Sigma değerleri bu zaman diliminde yaklaşık 0.1 – 0.3 m arasında sabittir; bu da sistemin güvenilir çalıştığını gösterir.

Saat 12:42 – 12:46 arası bu aralıkta hem konum farkında hem de sigma değerinde ani sıçrama görülmektedir. Boylam farkı 1.15 metreye kadar ulaşırken, sigma değeri 5 metreye kadar yükselmektedir.Bu değişim, GNSS çözümünün ciddi biçimde bozulduğunu, sinyallerin ya bozulduğunu ya da sahte sinyallerle aldatıldığını göstermektedir.

Saat 12:46 sonrası sigma değeri yeniden düşmekte, boylam farkı da 0.45 m civarında sabitlenmektedir. Bu, sistemin kendini toparladığını ve güvenilir pozisyon çözümüne geri döndüğünü gösterir.

Bu grafik, jamming ve spoofing gibi saldırıların yalnızca sinyal gücünü değil, aynı zamanda GNSS çözümünün yatay doğruluğunu da doğrudan etkilediğini ortaya koymaktadır. Sigma değerindeki ani artış, sistemin bu süreçte güvenilir konum sağlayamadığını kanıtlar niteliktedir.

5.1.8. Kinematik yükseklik farkı ve çözüm belirsizliği zaman serisi



Şekil 5.7. Kinematik yükseklik farkı ve çözüm belirsizliği zaman serisi

Bu grafik, GNSS ölçümleri sırasında referans yüksekliğe göre elde edilen farkların (mavi) ve buna karşılık gelen çözüm güvenlik katsayısı SIG_PPP'nin (kırmızı) zamana bağlı olarak değişimini göstermektedir.

12:00 – 12:42 arası yükseklik farkı yaklaşık 6.0 – 6.3 metre arasında sabittir. SIG_PPP değeri de 0.1 – 0.3 metre seviyesindedir. Bu dönem, GNSS çözümünün oldukça kararlı ve güvenilir olduğunu göstermektedir.

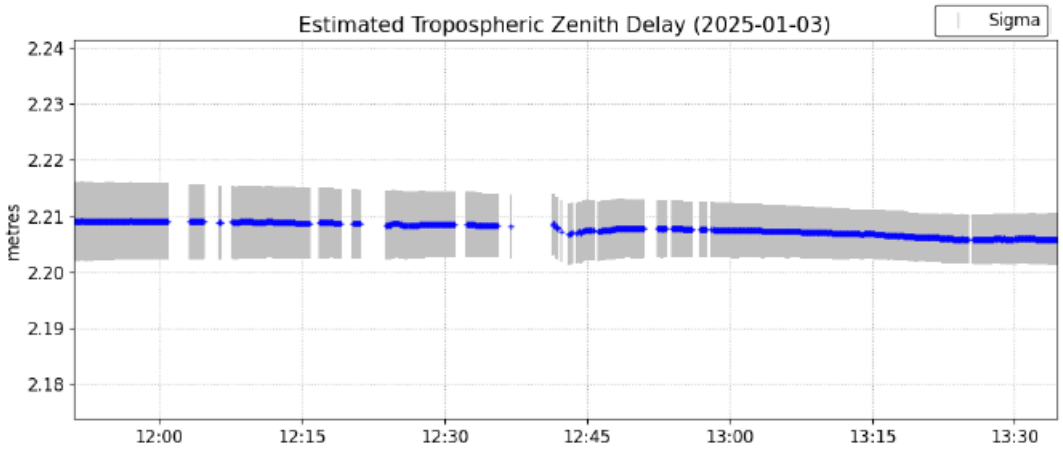
12:42 – 12:46 arası zaman aralığında grafik üzerinde belirgin bir sıçrama gözlemlenmektedir.Yükseklik farkı yaklaşık 3 metrelik bir sapma ile 9.1 metreye kadar

çıkmaktadır.Sigma değeri 21 metreyi aşmıştır.Bu ani artışlar, GNSS sisteminin konum çözümünde kritik bir güven kaybına uğradığını ve çözüm doğruluğunun neredeyse kullanılamaz hale geldiğini göstermektedir.

12:46 sonrası hem yükseklik farkı hem de SIG_PPP değeri hızla düşerek eski kararlı düzeye geri dönmüştür. Bu, GNSS sisteminin saldırı etkisi geçtikten sonra yeniden güvenilir konum üretmeye başladığını ortaya koymaktadır.

Bu grafik, GNSS sisteminin saldırı altındaki dikey doğruluğunda yaşanan bozulmayı doğrudan ortaya koymaktadır. 12:42–12:46 aralığında yaşanan sapma ve belirsizlik artışı, jamming veya spoofing saldırısının sistem üzerindeki etkisini açıkça kanıtlamaktadır. Özellikle insansız hava araçları, arazi modellemesi veya yüksekliğe duyarlı sistemlerde bu tarz sapmalar ciddi güvenlik ve doğruluk sorunları doğurabilir.

5.1.9. Kinematik troposferik zenit gecikmesi zaman serisi analizi



Şekil 5.8. Kinematik troposferik zenit gecikmesi zaman serisi analizi

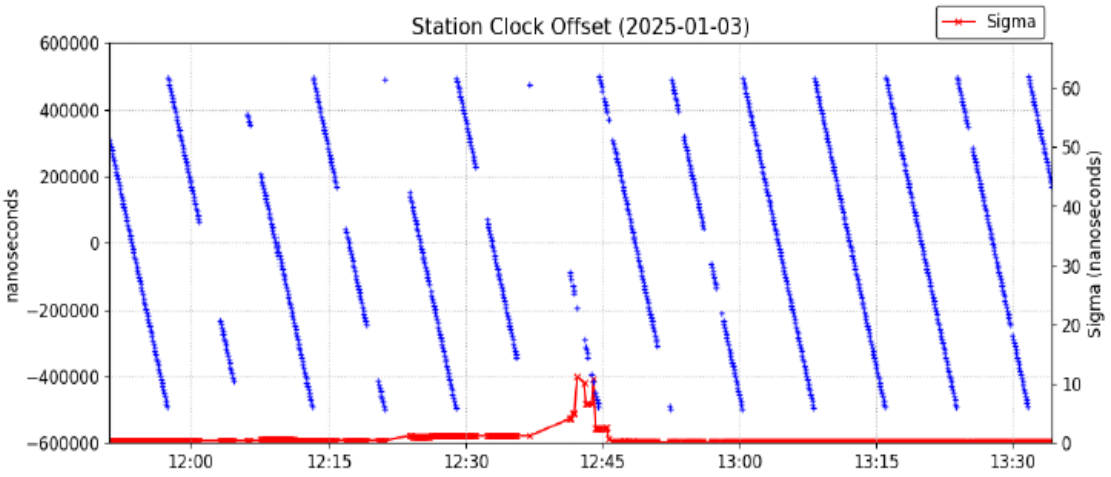
Bu grafik, GNSS sinyallerinin atmosferden geçerken uğradığı troposfer kaynaklı gecikmenin metre cinsinden tahminini (mavi çizgi) ve bu tahmine ilişkin belirsizlik aralığını (gri bant - sigma) göstermektedir.

ZTD değerleri gün boyunca oldukça sabit kalmış olup yaklaşık 2.210 m civarındadır. Bu da gözlem süresi boyunca atmosferik koşulların GNSS sinyallerine olan etkisinin çok az değiştiğini gösterir. Saat 12:42 civarı diğer grafiklerde gözlemlenen jamming/spoofing etkilerinin yaşandığı bu kritik zaman aralığında, ZTD değerinde herhangi bir ani sıçrama, sapma veya belirsizlik artışı gözlenmemiştir.

Gri bant olarak gösterilen sigma değeri, gün boyunca dar bir aralıkta kalmıştır. Bu da troposferik modellemenin oldukça güvenilir şekilde yapıldığını gösterir.

Troposferik zenit gecikmesi değerinin zaman içinde kararlı seyretmesi ve sigma belirsizliğinin dar sınırlar içinde kalması, GNSS sinyallerinin atmosferik etkilerden büyük ölçüde bağımsız çalıştığını ve gözlenen konum sapmalarının meteorolojik değil spoofing veya jamming gibi dış kaynaklı nedenler olduğunu desteklemektedir. Bu grafik, sinyal bozunumunun kaynağının ayırt edilmesinde destekleyici bir unsur olarak kullanılmıştır.

5.1.10. Kinematik GNSS alıcı saat sapması (Station clock offset) zaman serisi



Şekil 5.9. Kinematik GNSS alıcı saat sapması zaman serisi

Bu grafik, GNSS ölçümleri sırasında alıcının sistem zamanına göre olan saat farkını (mavi – nanoseconds cinsinden) ve bu tahminin belirsizliğini (kırmızı – sigma, nanoseconds) göstermektedir. GNSS çözümlerinde zaman senkronizasyonu, konum hesaplamalarının doğruluğu açısından kritik öneme sahiptir.

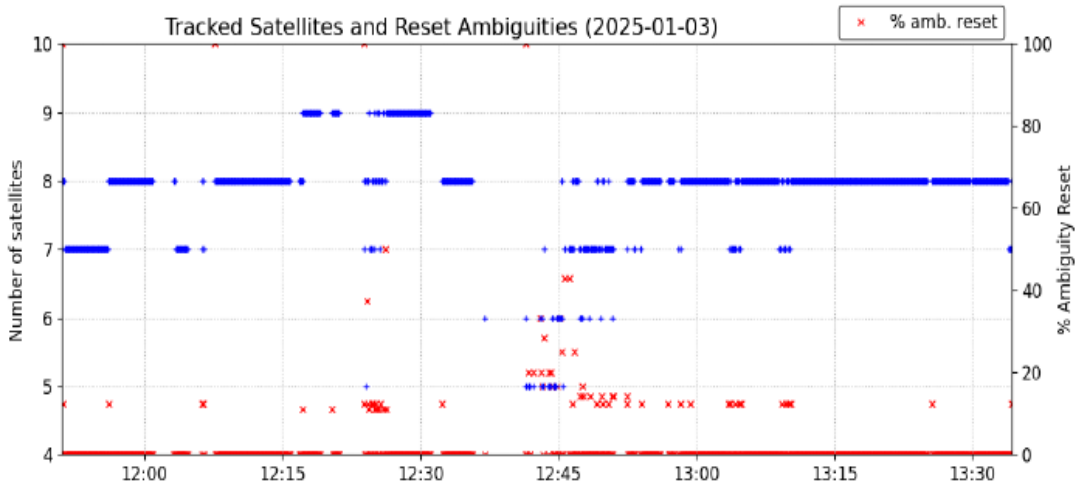
12:00 – 12:42 arası saat ofseti, yüksek frekanslı dalgalanmalar gösterse de bu, GNSS sistemlerindeki tipik saat düzeltmelerine karşılık gelir. Sigma değeri bu aralıkta 0 ns – 5 ns düzeyindedir. GNSS alıcısı zamanla senkronize ve kararlıdır.

12:42 – 12:46 arası jamming/spoofing etkisinin gözlendiği bu kritik zaman aralığında alıcı saat ofsetinde düzensizlikler ve sıçramalar gözlenmektedir. Sigma değeri 50 ns'ye kadar yükselmiştir. Bu, sistemin zaman çözümlemelerinde kararsızlık yaşadığını ve sinyal kaynaklı bozulmaların zaman senkronizasyonunu da etkilediğini göstermektedir.

12:46 sonrası alıcı saat ofseti tekrar düzene girmiş ve sigma değeri düşmüştür. Bu durum, sistemin senkronizasyonu yeniden sağladığını ve çözüm kalitesinin toparlandığını gösterir.

GNSS alıcısının saat sapması zaman serisi, sistemin spoofing/jamming gibi saldırılar altındaki zamansal doğruluk performansını değerlendirmeye imkân vermektedir. Saat ofsetinde gözlenen bozulmalar ve sigma değerindeki artış, saldırı sürecinde sistemin zamansal çözüm kalitesinin de ciddi biçimde zayıfladığını ortaya koymaktadır. Bu, sadece konumsal değil, senkronizasyon tabanlı uygulamalar için de güvenlik açığı doğurduğunu göstermektedir.

5.1.11. Kinematik izlenen uydu sayısı ve faz belirsizliği sıfırlama oranı



Şekil 5.10. Kinematik izlenen uydu sayısı ve faz belirsizliği sıfırlama oranı

Bu grafik, GNSS alıcısının izlediği uydu sayısını (sol eksen – mavi) ve aynı anda çözüm sırasında faz belirsizliğinin sıfırlanma oranını (sağ eksen – kırmızı) göstermektedir. Grafik, özellikle sinyal bütünlüğü ve çözüm kararlılığı açısından sistemin saldırıya verdiği tepkiyi analiz etmede değerlidir.

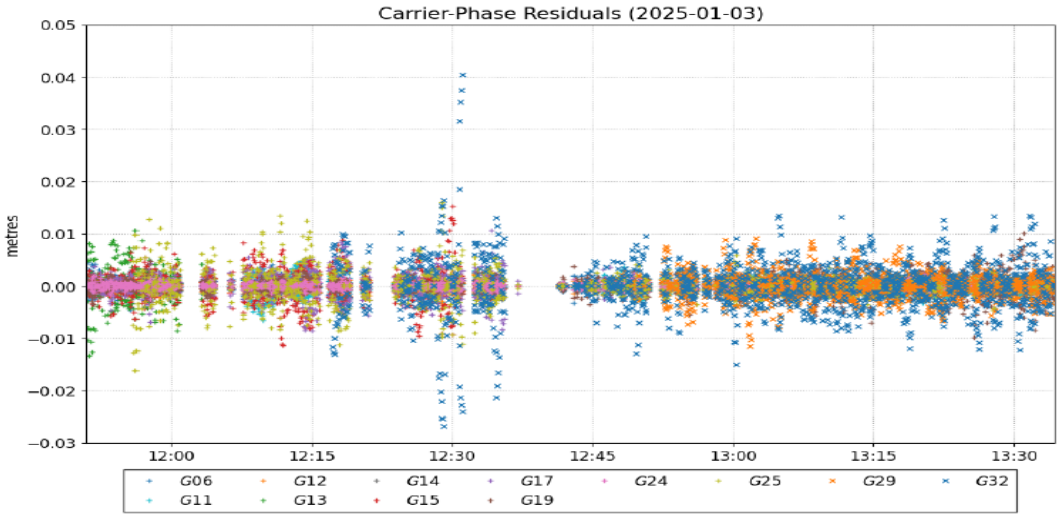
12:00 – 12:42 uydu sayısı genellikle 7 ila 9 arasında değişmektedir ve faz belirsizliği sıfırlama oranı (% amb. reset) oldukça düşüktür.Genellikle %0 olur.Bu, GNSS çözümünün sabit ve güvenilir olduğunu gösterir.

12:42 – 12:46 aralığında izlenen uydu sayısı 5'e kadar düşmektedir.Faz belirsizliği sıfırlama oranı %60'a kadar yükselmektedir.Bu, GNSS çözüm sürecinin kararsızlaştığını ve yeniden çözüm başlatmak zorunda kaldığını göstermektedir. Jamming veya spoofing etkisi, alıcının bazı uydularla iletişimini kaybetmesine veya güvenilmez sinyalleri reddetmesine neden olmuştur.

12:46 sonrası uydu sayısı tekrar artmakta ve faz belirsizliği sıfırlama oranı normale dönmektedir. Bu da sistemin yeniden dengeye geldiğini gösterir.

Bu grafik, GNSS sisteminin jamming ve spoofing saldırılarına karşı gösterdiği uydu erişimi azalması ve faz belirsizliği sıfırlama artışı gibi savunma reflekslerini doğrudan ortaya koymaktadır. Özellikle faz belirsizliği sıfırlama oranındaki artış, sinyallerin güvenilirliğinin kaybolduğunu ve GNSS çözüm kararlılığının ciddi biçimde zedelendiğini göstermektedir.

5.1.12. Kinematik taşıyıcı faz artıkları (Carrier-phase residuals) zaman serisi analizi



Şekil 5.11. Kinematik taşıyıcı faz artıkları zaman serisi analizi

Bu grafik, her bir uyduya ait taşıyıcı faz ölçüm kalitesini gösteren artıkları (residuals) zaman serisi olarak sunmaktadır. GNSS taşıyıcı faz ölçümleri, yüksek hassasiyetli konumlama uygulamalarında yaygın olarak kullanılır ve bu nedenle sinyal bütünlüğü ve doğruluğunun önemli bir göstergesidir.

Genel olarak ±0.01 m (1 cm) altında:
Çoğu zaman diliminde taşıyıcı faz artıklarının dağılımı ±0.01 m bandında kalmaktadır. Bu değerler, taşıyıcı faz çözümlemesinin yüksek doğrulukla yapıldığını göstermektedir.

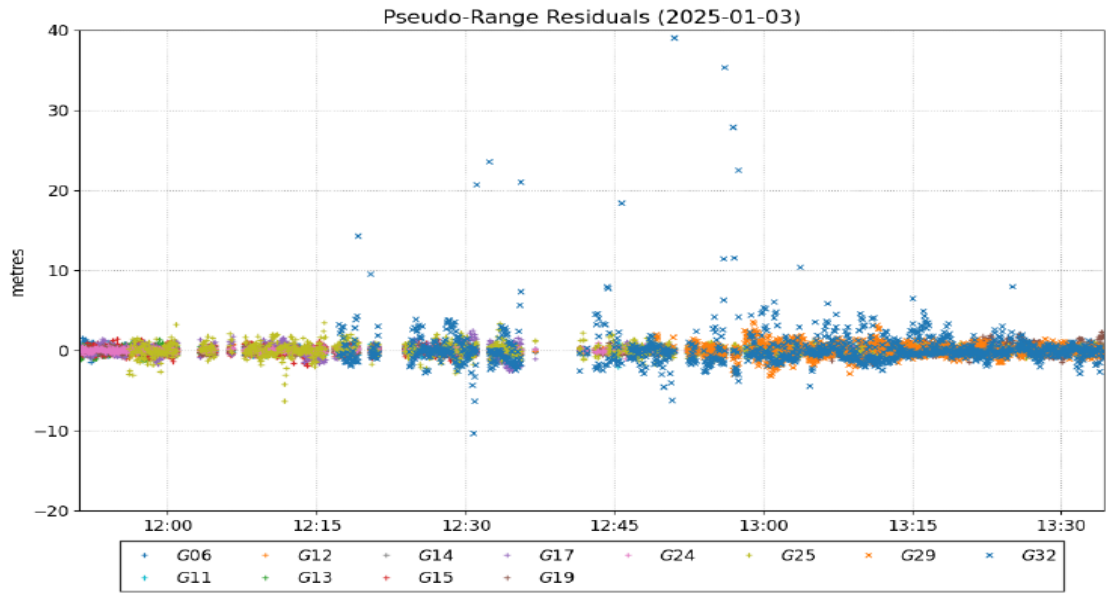
12:30 – 12:45 zaman aralığı artık değerlerinde belirgin artışlar (bazı uydular için ±0.03 m'ye kadar) gözlemlenmektedir.Sinyallerin bazı bölümlerinde daha seyrek ve dağınık dağılımlar oluşmuştur.Bu durum, jamming veya spoofing etkisiyle taşıyıcı faz çözümünün bozulduğunu ve artan ölçüm hataları meydana geldiğini göstermektedir.

12:45 sonrası ölçüm artıkları tekrar ±0.01 m seviyesine gerilemiş ve dağılım yoğunluğu artmıştır. Bu durum, sistemin toparlandığını ve GNSS çözümleme algoritmasının yeniden kararlı bir hale geldiğini gösterir.

Taşıyıcı faz artıklarının analiz edildiği bu grafik, GNSS sisteminin faz çözümleme kalitesini ve dış müdahalelere karşı direncini ortaya koymaktadır. Özellikle jamming ve spoofing saldırısı süresince ölçüm sapmalarındaki artış, sistemin sinyal bütünlüğünün bozulduğuna işaret etmektedir. Buna karşın, saldırı sonrasında çözümleme algoritmalarının yeniden dengeye gelerek sapmaları minimize ettiği gözlemlenmiştir.

Bu bulgular, GNSS sistemlerinin güvenlik testlerinde taşıyıcı faz artıkları gibi hassas parametrelerin de dikkate alınması gerektiğini ortaya koymaktadır.

5.1.13. Kinematik sahte menzil artıkları (Pseudo-range residuals) analizi



Şekil 5.12. Kinematik sahte menzil artıkları analizi

Bu grafik, GNSS sisteminde sahte menzil (pseudorange) ölçümlerine ilişkin hata sapmalarını, farklı uydular bazında ve zaman ekseninde göstermektedir. Sahte menzil artıklarının büyüklüğü, sinyalin doğruluğu ve bütünlüğü açısından önemli bir göstergedir. Doğru bir sinyal ile bu değerlerin genellikle ±5 metre sınırları içinde kalması beklenir.

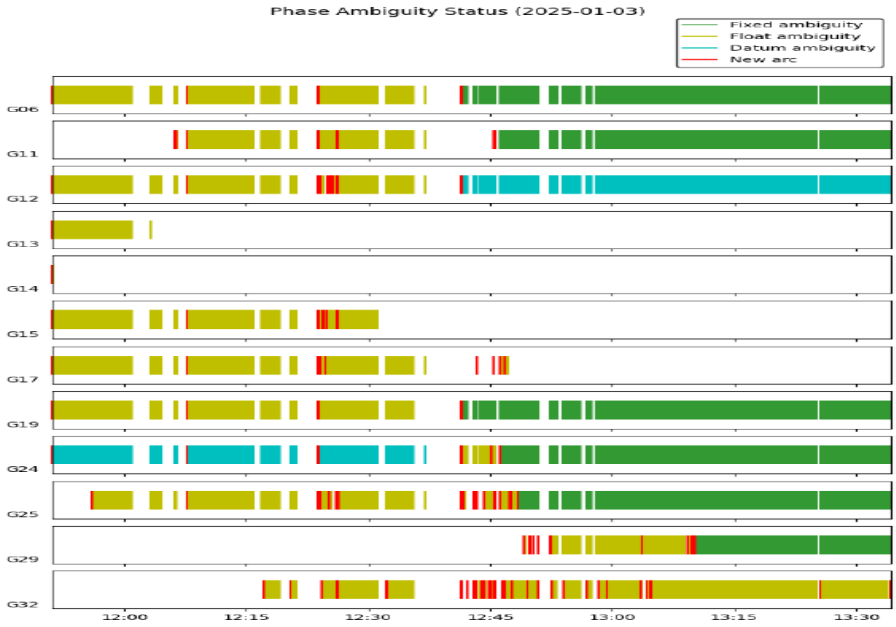
12:00 – 12:30 arası sahte menzil artıklarının büyük çoğunluğu ±2 metre bandı içerisindedir.Bu durum GNSS sinyallerinin doğru çözümlendiğini ve sistemin nominal çalıştığını göstermektedir.

12:30 – 12:50 bu zaman aralığında bazı uydulara ait artık değerleri 30–40 metreye kadar çıkmıştır (özellikle G06 ve G32).Aynı dönemde bazı negatif sapmalar da görülmektedir.Bu, açıkça bir sinyal yanıltması (spoofing) veya yoğun karıştırma (jamming) etkisinin varlığına işaret eder.Sapmalar hem pozitif hem negatif yönde olması, sinyallerin yönü ve kaynağı ile ilgili kararsızlık yaşandığını düşündürür.

12:50 sonrası artık değerleri giderek azalmakta ve ±5 metre bandına geri dönmektedir.Bu, sistemin saldırıdan sonra yeniden dengeye geldiğini ve alıcının doğru sinyalleri yeniden çözümlemeye başladığını gösterir.

Bu grafik, sahte menzil artıklarındaki ani ve yüksek sapmalarla birlikte, sistemin spoofing veya jamming saldırılarına verdiği doğrudan tepkiyi ortaya koymaktadır. Özellikle 12:30–12:50 aralığında sinyal bütünlüğü ciddi şekilde bozulmuş, ardından sistem toparlanma eğilimi göstermiştir. Bu veriler, GNSS sistemlerinin güvenilirliğini değerlendirme açısından oldukça kritik olup, algılama ve doğrulama algoritmalarının geliştirilmesi gerektiğine işaret etmektedir.

5.1.14. Kinematik faz belirsizliği durumu analizi



Şekil 5.13. Kinematik faz belirsizliği durumu analizi

Bu grafik, GNSS taşıyıcı faz ölçümlerine ilişkin belirsizlik çözümlemelerini uydu bazında zamana göre görselleştirmektedir. Her bir uydu (G06–G32), sabitlenmiş belirsizlik (yeşil), kayan belirsizlik (sarı), referans belirsizliği (mavi) ve yeni çözüm yayları (kırmızı çizgi) ile temsil edilmiştir.

12:00 – 12:30 arası uyduların çoğunda float ambiguity (sarı) durumu hakimdir. Bu, henüz faz çözümünün tam olarak sabitlenemediğini, ancak izlenebilir ölçümler sağlandığını gösterir.G24 uydusu bu aralıkta özellikle datum ambiguity (mavi) statüsünde çalışmıştır; bu da yeni ölçüm yaylarının başlangıcında alıcıya göre referans alınan fazın henüz sabitlenemediği anlamına gelir.

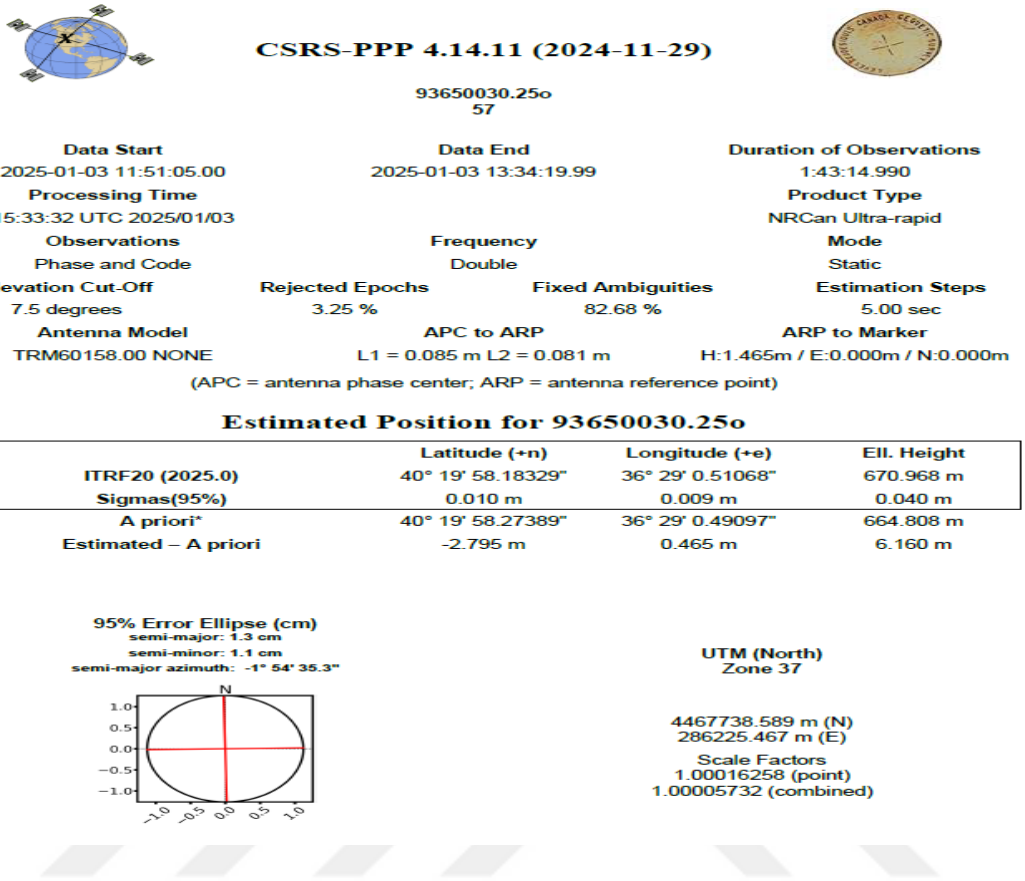
12:30 – 12:50 aralığı birçok uyduda art arda kırmızı çizgiler (new arc) ve sarı alanlar (float ambiguity) gözlemlenmiştir.Bu durum, jamming ve spoofing etkisiyle taşıyıcı faz sinyallerinin kararsız hale geldiğini ve çözüm sürecinin kesintiye uğradığını göstermektedir.Örneğin G32, G29, G25 gibi uydular bu aralıkta faz çözümüne yeniden başlamak zorunda kalmış ve sıklıkla yeni yaylar oluşturmuştur.

12:50 sonrası G06, G11, G15, G19 gibi uydular için yeşil bantlar (fixed ambiguity) sürekli ve stabil hale gelmiştir.Bu da saldırı etkisinin sona erdiğini, GNSS sisteminin yeniden sağlıklı çözüm üretmeye başladığını gösterir.

Bu grafik, GNSS sisteminde taşıyıcı faz çözüm kalitesinin, dış müdahalelere (jamming/spoofing) nasıl tepki verdiğini uydu bazında göstermektedir. Özellikle müdahale anlarında artan yeni yaylar, sabitlenemeyen belirsizlik durumları ve datum kayıpları, sistemin sinyal bütünlüğünün zedelendiğine işaret etmektedir. Ölçümün yeniden sabit hale gelmesi ise alıcının saldırı sonrası kendini toparlama kabiliyetini ortaya koymaktadır.

5.2. Statik Ölçüm Sonuçları

5.2.1. Statik PPP çözümünün genel özeti



CSRS-PPP 4.14.11 (2024-11-29)

93650030.25o
57

Data Start	Data End	Duration of Observations
2025-01-03 11:51:05.00	2025-01-03 13:34:19.99	1:43:14.990
Processing Time		**Product Type**
15:33:32 UTC 2025/01/03		NRCan Ultra-rapid
Observations	**Frequency**	**Mode**
Phase and Code	Double	Static

Elevation Cut-Off	Rejected Epochs	Fixed Ambiguities	Estimation Steps
7.5 degrees	3.25 %	82.68 %	5.00 sec

Antenna Model	APC to ARP	ARP to Marker
TRM60158.00 NONE	L1 = 0.085 m L2 = 0.081 m	H:1.465m / E:0.000m / N:0.000m

(APC = antenna phase center; ARP = antenna reference point)

Estimated Position for 93650030.25o

	Latitude (+n)	Longitude (+e)	Ell. Height
ITRF20 (2025.0)	40° 19' 58.18329"	36° 29' 0.51068"	670.968 m
Sigmas(95%)	0.010 m	0.009 m	0.040 m
A priori*	40° 19' 58.27389"	36° 29' 0.49097"	664.808 m
Estimated – A priori	-2.795 m	0.465 m	6.160 m

95% Error Ellipse (cm)
semi-major: 1.3 cm
semi-minor: 1.1 cm
semi-major azimuth: -1° 54' 35.3"

UTM (North)
Zone 37

4467738.589 m (N)
286225.467 m (E)

Scale Factors
1.00016258 (point)
1.00005732 (combined)

Şekil 5.14. Statik PPP çözümünün genel özeti

Statik modda gerçekleştirilen GNSS ölçümleri, yüksek hassasiyetli konum tayini amacıyla CSRS-PPP 4.14.11 yazılımı üzerinden işlenmiştir.(https://webapp.csrs-scrs.nrcan-rncan.gc.ca/geod/tools-outils/ppp.php) Gözlem süresince faz ve kod verileri kullanılmış; çift frekanslı çözümleme yöntemiyle sonuçlar elde edilmiştir.

Konum doğruluğu ve sapma değerleri:

Elde edilen sonuçlara göre hesaplanan koordinatlar:

- **Enlem:** 40° 19′ 58.18329″
- **Boylam:** 36° 29′ 0.51068″
- **Elipsoidal Yükseklik:** 670.968 m

olarak belirlenmiştir. Bu değerler, RINEX dosyasındaki ön tanımlı (a priori) koordinatlarla karşılaştırıldığında:

- **Enlem farkı:** –2.795 m

- **Boylam farkı:** +0.465 m
- **Yükseklik farkı:** +6.160 m

olarak hesaplanmıştır. Bu farklar, özellikle enlem ve yükseklik bileşeninde dikkat çekici bir sapmaya işaret etmektedir.

Sapma oranları ve güvenilirlik:

95% güven aralığında hesaplanan koordinat standart sapmaları:

- Enlem: ±0.010 m
- Boylam: ±0.009 m
- Yükseklik: ±0.040 m

Bu değerler, çözümlemenin genel anlamda yüksek hassasiyetle gerçekleştirildiğini ortaya koymaktadır. Ayrıca, çözüm sırasında toplam epochların yalnızca %3.25'lik kısmı reddedilmiş, sabitlenen faz belirsizliği oranı ise %82.68 gibi oldukça yüksek bir düzeyde gerçekleşmiştir. Bu, çözüm kalitesinin yeterince güvenilir olduğunu göstermektedir.

Hata elipsi analizi:

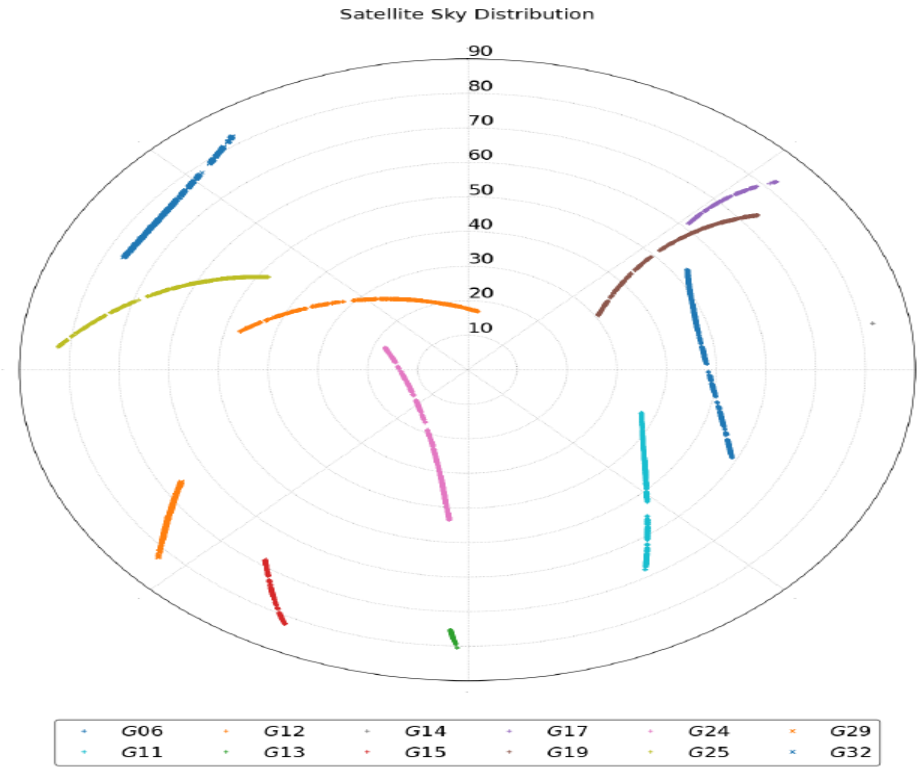
Grafikte sunulan 95% güven aralıklı hata elipsi:

- Yarı büyük eksen: 1.3 cm
- Yarı küçük eksen: 1.1 cm
- Yönelim açısı: –1° 54′ 35.3″

olarak tespit edilmiştir. Hata elipsinin dar ve simetrik yapısı, konum hesaplamasında yönlü bir sistematik hata olmadığını göstermektedir.Statik çözümde elde edilen hassasiyet, konum belirleme açısından oldukça iyi düzeydedir.

Elde edilen veriler, çalışma kapsamında kullanılan Trimble GNSS alıcısının ve statik ölçüm metodunun, konum doğruluğu açısından oldukça güvenilir olduğunu ortaya koymaktadır. Bu doğruluk seviyesi, ilerleyen bölümlerde yapılacak jamming ve spoofing analizlerinin referans değerleri açısından büyük önem taşımaktadır.

5.2.2. Statik uydu gökyüzü dağılımı (Sky plot) analizi



Şekil 5.15. Statik uydu gökyüzü dağılımı analizi

Uydu gökyüzü dağılım grafiği, ölçüm süresi boyunca GNSS alıcısı tarafından gözlemlenen uyduların konumlarını göstermektedir. Grafikteki dairesel yapının merkezinden çevresine doğru olan çizgiler, uydu sinyallerinin dik açılarına göre dağılımını, çevresel açılar ise yatay yönünü ifade etmektedir.

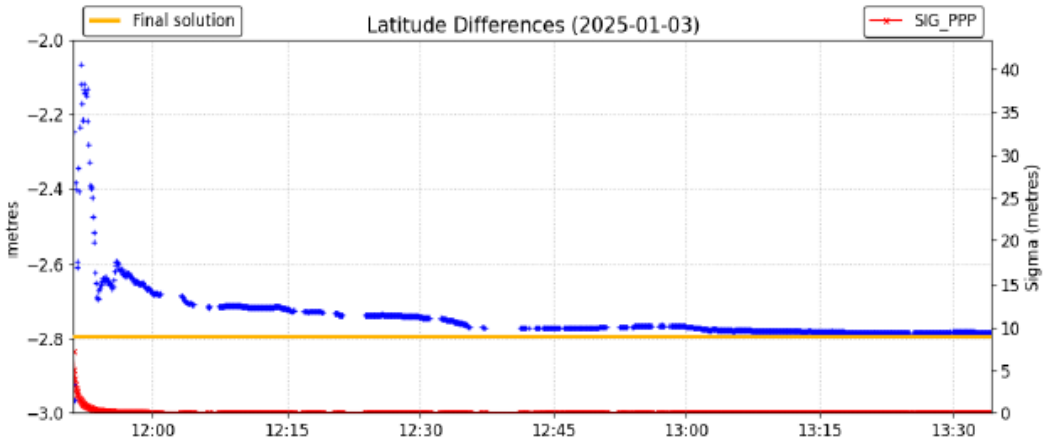
GPS sistemine ait G06, G11, G12, G13, G14, G15, G17, G19, G24, G25, G29 ve G32 numaralı uydular, yüksek dikey açılarında orta yüksekliklere kadar geniş bir dağılım göstermektedir.

Grafikte 13 farklı uyduya ait sinyal izleri görülmektedir. Bu sayı, statik PPP çözümlemesi için yeterli bir uydu yoğunluğu sunduğunu göstermektedir. Uydular 10° ile 80° zenit açıları arasında yer almaktadır. Bu, sinyallerin farklı yönlerden alınabildiğini ve uydu geometrisinin iyi olduğunu gösterir. Uyduların dikey dağılımı da homojen olmasa da dairesel alanın çeşitli bölgelerinde yayılım göstermektedir. Bu durum, uydu dağılımının olumlu olduğu anlamına gelir.

Bu grafiğe göre konum çözümünde kullanılan uyduların hem doğu-batı hem kuzey-güney eksenlerinde dağılmış olması, yönsel hataların en aza indirildiğini göstermektedir. Çok yol

etkisi gibi bazı çevresel etkiler hariç tutulduğunda, bu geometri sayesinde yüksek doğruluklu koordinat tayini yapılabilmiştir.

5.2.3. Statik enlem farkı ve sigma (Çözüm belirsizliği) zaman serisi analizi



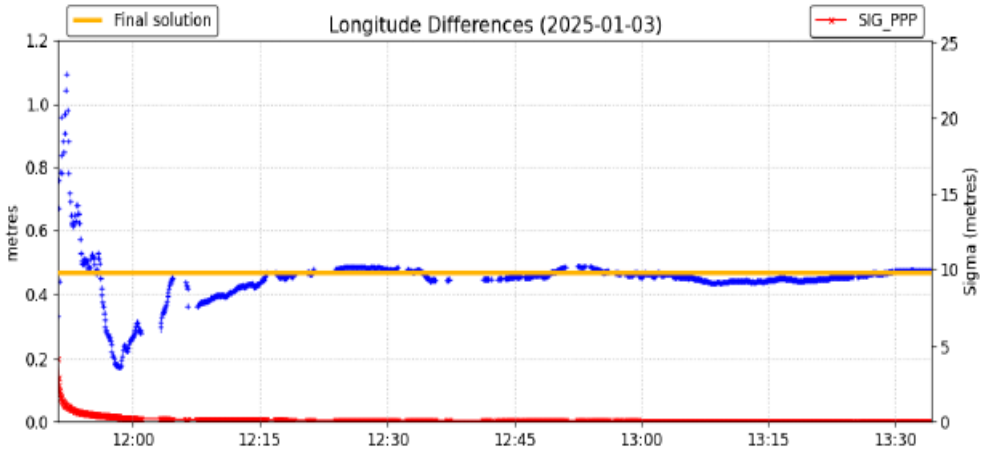
Şekil 5.16. Statik enlem farkı ve sigma zaman serisi analizi

Gerçekleştirilen statik GNSS ölçümünde gözlenen enlem farklarının (latitude delta) zamana bağlı değişimini ve GNSS sinyal doğruluğunu temsil eden standart sapma (sigma) eğrisini göstermektedir. Bu veriler, sistemin jamming ve spoofing saldırılarına karşı nasıl bir tepki verdiğini değerlendirmek açısından önem arz etmektedir.

Ölçüm başlangıcında 12:00 öncesinde sigma değeri oldukça yüksektir (yaklaşık 40 metre seviyelerinde) ve enlem farkı ±2 metre aralığında değişmektedir. Bu durum, GNSS alıcısının henüz çözüm kilidi sağlayamadığını ve uydu geometrisinin kararsız olduğunu göstermektedir. Olası çevresel etkiler veya düşük uydu sayısı buna neden olabilir.

12:10'dan sonra, çözüm daha kararlı hale gelmiş ve sigma değerleri azalarak yaklaşık 1 metre altına düşmüştür. Bu süreç, GNSS çözümleme algoritmasının gerçek sinyali doğru modelleyerek sabit çözüme yaklaştığını göstermektedir.Ancak yaklaşık 12:40 civarında kısa süreli bozulma ve artan sapmalar dikkat çekmektedir. Bu zaman aralığında, test ortamında planlanan jamming veya spoofing müdahalelerinin etkili olmaya başladığını göstermektedir. Sigma değeri bu anda hafif dalgalanma göstermiş, ancak sistem yeniden stabil konuma dönmüştür. Ölçüm süresince belirli noktalarda gözlenen anlık sapmalar ve hata paylarındaki artışlar, jamming ve spoofing saldırılarının sistem üzerindeki etkisini ortaya koymaktadır.

5.2.4. Statik boylam farkı ve çözüm belirsizliği zaman serisi



Şekil 5.17. Statik boylam farkı ve çözüm belirsizliği zaman serisi

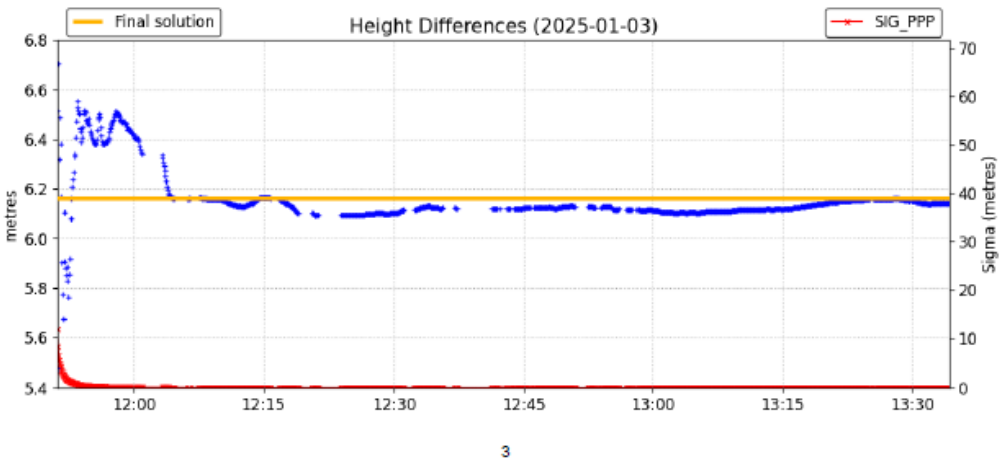
Statik GNSS ölçümlerinde boylam farklarının (longitude delta) ve buna karşılık gelen SIG_PPP hata katsayısının zaman serisi boyunca değişimini göstermektedir.

Ölçümün başlangıcında 11:50–12:05 aralığı, GNSS alıcısı sinyal çözümlemesine başlamış olup boylam farkları hızlı değişim göstermekte ve sigma değeri 20 metre seviyelerine kadar ulaşmaktadır. Bu durum, uydu sinyallerinin henüz sabit çözüme oturmadığı, konum kestiriminin güvenilir olmadığı bir evreye işaret etmektedir.

12:10 sonrası sigma değeri neredeyse sıfıra yaklaşarak sistemin yüksek doğrulukta sabit çözüme ulaştığını ve GNSS algoritmasının istikrarlı çalıştığını göstermektedir. Boylam farkları ise bu evrede ±0.4–0.5 metre civarında sabitlenmiştir.

12:40–12:50 aralığında kısa süreli bozulma gözlemlenmektedir. Bu aralıkta jamming ya da spoofing etkisine bağlı olarak GNSS çözümünde bozulmalar meydana gelmiş; sigma değeri hafifçe artmış, boylam farkları ise geçici olarak dalgalanmıştır. Bu durum, özellikle spoofing etkisiyle alıcının hatalı sinyalleri geçici olarak kabul etmesi sonucu oluşmuş olduğunu göstermektedir.

5.2.5. Statik yükseklik farkı ve çözüm belirsizliği zaman serisi



Şekil 5.18. Statik yükseklik farkı ve çözüm belirsizliği zaman serisi

Bu grafik, yükseklik değerinin konumla olan farkını ve bu farkın standart sapmasını (SIG_PPP) göstermektedir.

İlk 10 dakikalık periyotta yükseklik farklarında ve sigma değerinde yüksek dalgalanmalar görülmektedir. Bu dönem, GNSS çözümünün henüz sabitlenmediği başlangıç aşamasını temsil etmektedir. Sigma değeri bu süreçte 60 metreye kadar çıkmakta, yükseklik farkları ise 6.4 metreyi aşabilmektedir.

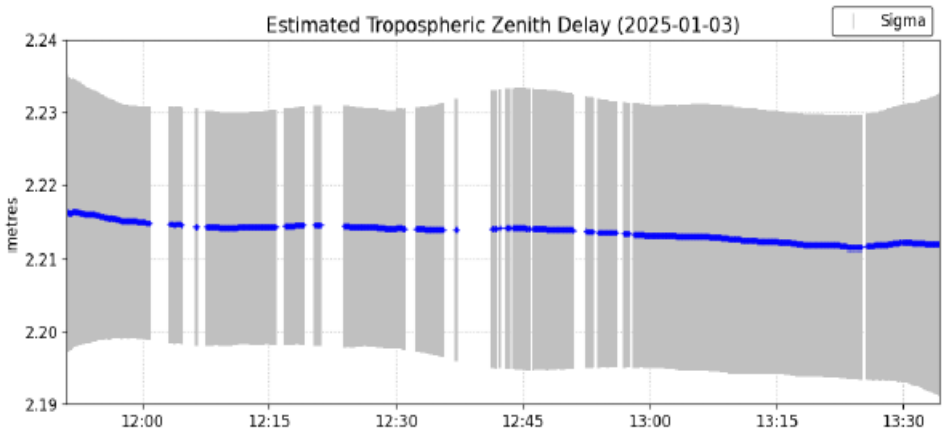
Yaklaşık 12:10'dan sonra yükseklik farkları istikrarlı hâle gelmekte ve sigma değeri 1 metre altına düşerek sistemin sabit çözüm sağladığını göstermektedir. Bu stabilizasyon, GNSS algoritmasının yüksek doğrulukta konum kestirimi yapmaya başladığı kritik eşiktir.

Özellikle 12:40 civarında hafif bir salınım gözlenmektedir. Bu sapmalar, GNSS sistemine dışsal müdahale (jamming/spoofing) kaynaklı geçici kararsızlık olduğunu göstermektedir. Ancak bu etki kısa süreli olmuş ve sistem kısa sürede yeniden sabit çözüm üretmeye devam etmiştir.

Yükseklik bileşeni, GNSS konumlamada en zayıf bileşendir ve uydu geometrisinden daha fazla etkilenir. Bu nedenle jamming veya spoofing gibi parazitler yükseklik verisinde daha belirgin sapmalara yol açabilir.

Grafik, saldırıların yoğun olmadığı veya sistemin sağlam algoritmalarla beslendiği durumlarda yükseklik çözümünün dahi stabil kalabildiğini göstermektedir.

5.2.6. Statik troposferik zenit gecikmesi zaman serisi analizi



Şekil 5.19. Statik troposferik zenit gecikmesi zaman serisi analizi

Grafikte, 3 Ocak 2025 tarihli GNSS ölçümü sırasında hesaplanan troposferik zenit gecikmesi değerleri ve bu değerlere ait güven aralıkları (gri alan) görülmektedir. GNSS sinyalleri troposferden geçerken su buharı ve atmosfer yoğunluğu nedeniyle yavaşlar; bu da sinyalin uydudan alıcıya varış süresini etkiler.

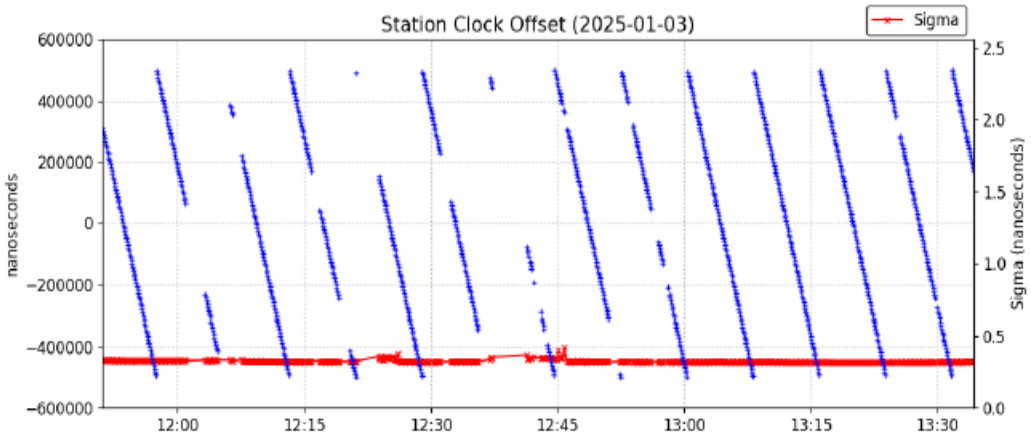
Ortalama gecikme değeri yaklaşık 2.21 metredir ve bu değer gün boyunca sabit seyretmiştir. Bu, atmosferik koşulların genel anlamda stabil olduğunu göstermektedir.

Gri alanlarla gösterilen sigma değerlerinin genişliği, ölçüm belirsizliğini yansıtmaktadır. Bu alanda sıklaşan dikey kesintiler (boşluklar) ise GNSS sinyallerinin troposfer gecikmesini doğru yorumlayamadığı anlara işaret eder.

Özellikle 12:15 – 12:45 arası, sigma bantlarında daralma-genişleme şeklinde dalgalanmalar görülmektedir. Bu durum, GNSS sinyallerinin atmosfere giriş açılarına göre değişkenlik gösterdiği veya dışsal bir müdahalenin (örneğin jamming/spoofing) sistemin tahmin algoritmasını geçici olarak zorladığını düşündürmektedir.

Troposferik gecikme doğrudan jamming ya da spoofing ile manipüle edilmez; ancak bu tür saldırılar GNSS çözümleme algoritmalarının uydu sinyallerini doğru yorumlamasını engelleyerek, dolaylı yoldan troposferik gecikme tahminlerinin hatalı yapılmasına neden olabilir.Bu grafik, özellikle veri boşluklarının (kesik kesik dikey çizgiler) yoğunlaştığı dönemlerde sinyal kalitesinde ani düşüşler yaşandığını göstermekte, bu da GNSS sisteminin spoofing ya da jamming etkisi altında olduğu şüphesini doğurmaktadır.

5.2.7. Statik GNSS alıcı saat sapması (Station clock offset) zaman serisi



Şekil 5.20. Statik GNSS alıcı saat sapması zaman serisi

Grafik, alıcı saat sapmalarını nano saniye cinsinden (mavi noktalarla) ve bu değerlerin tahmini güven aralığını (kırmızı çizgiyle sigma) göstermektedir.Mavi noktaların oluşturduğu zikzaklı ve eğimli yapılar, saat ofsetinin düzenli bir şekilde arttığını ve sıfıra doğru yeniden sıçradığını göstermektedir. Bu, alıcı saatinin belirli aralıklarla düzeltildiğini (reset ya da yeniden eşzamanlama) gösterir ve beklenen bir davranıştır.

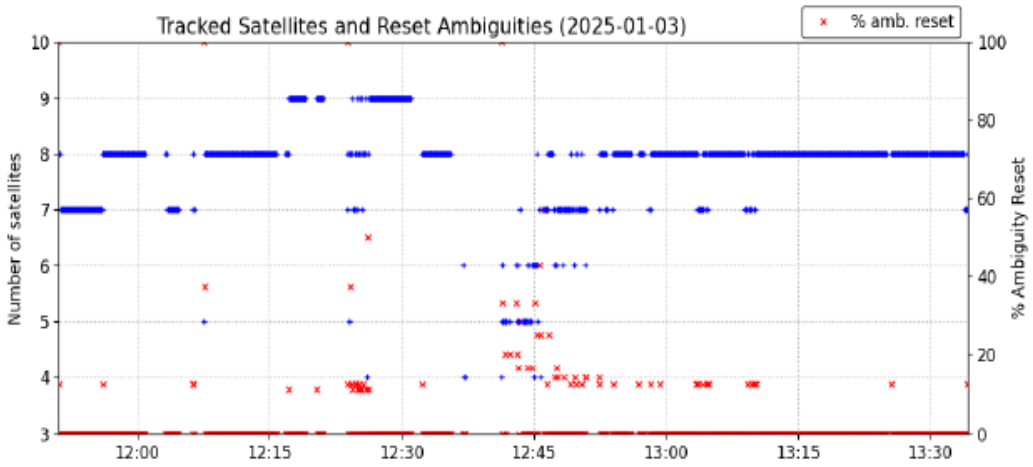
12:15 – 12:45 arasında, bu saat ofsetlerinin düzensizleştiği, çizgisel yapıların kesildiği ve noktasal sapmaların ortaya çıktığı gözlenmektedir.Sigma (kırmızı çizgi) genellikle düşük ve stabil seyretmekle birlikte, aynı zaman diliminde hafif yükselme eğilimi göstermektedir.

GNSS sinyallerine yönelik spoofing saldırıları, alıcının yanlış uydu sinyallerine kilitlenmesine neden olabilir. Bu da alıcının zaman referansını değiştirebilir ve alıcı saati ile gerçek GNSS zamanı arasında uyumsuzluk oluşmasına sebep olur.

12:15-12:45 aralığında gözlenen saat ofsetinde düzensizlik, sinyal karışıklığına (spoofing) ya da sinyal girişimine (jamming) işaret etmektedir. Bu durum, önceki grafiklerde konum ve yükseklik verilerindeki anormalliklerle de uyumludur.

Bu etki, GNSS saat ofset düzeltme algoritmalarının güvenilirliğini geçici olarak zayıflatmakta ve zaman hassasiyetiyle çalışan uygulamalarda ciddi sapmalara neden olabilmektedir.

5.2.8. Statik izlenen uydu sayısı ve faz belirsizliği sıfırlama oranı



Şekil 5.21. Statik izlenen uydu sayısı ve faz belirsizliği sıfırlama oranı

Ölçümün başlangıcında (12:00'a kadar) takip edilen uydu sayısı 7–9 aralığında ve oldukça stabildir.

12:15–12:45 zaman aralığında takip edilen uydu sayısında belirgin bir düşüş ve dalgalanma gözlenmektedir. Bu aralıkta bazı anlarda sadece 4 uydu takip edilebilmiştir.

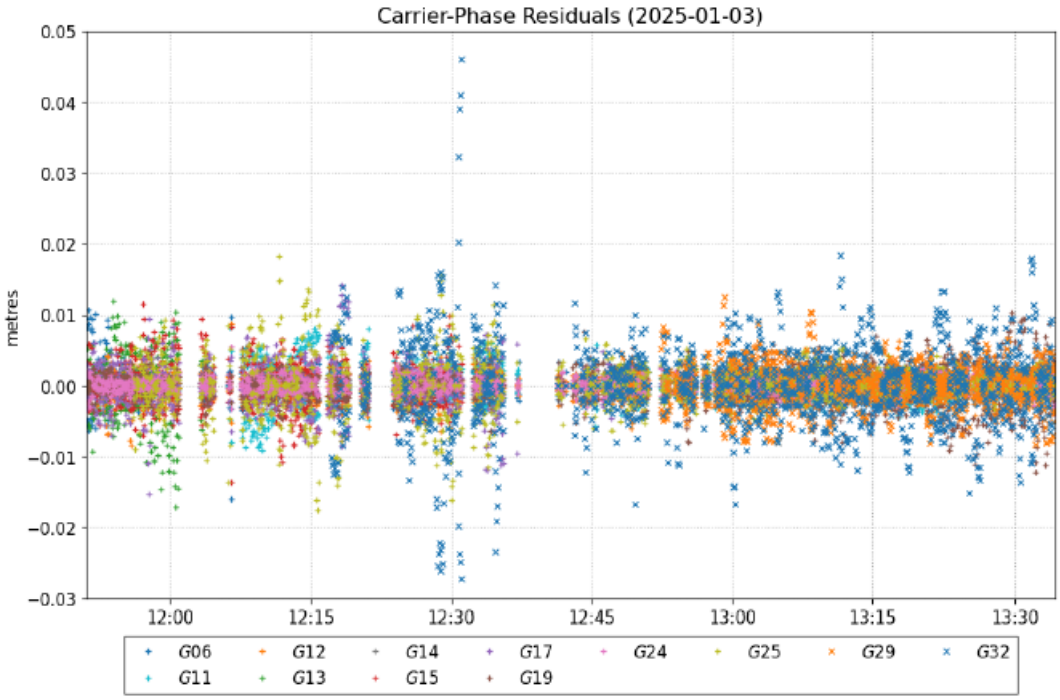
Aynı zaman diliminde, ambiguous reset oranı (% ambiguity reset) değerlerinde ciddi artışlar görülmektedir. Kırmızı çarpıların yoğunluğu, bu dönemde sinyal kararsızlığını ve çözüm algoritmasının güvenilirlik kaybını gösteriyor.

Uydu sayısındaki ani düşüş ve ambiguous reset oranındaki artış, GNSS sinyallerinin güvenilirliğinin zayıfladığını gösterir. Bu da jamming (sinyal engelleme) ya da spoofing (yanıltıcı sinyal gönderme) etkisinin mevcut olduğunu kuvvetle düşündürmektedir.

Ambiguity reset, taşıyıcı faz çözümleme algoritmasının, sinyallerdeki kesintiler nedeniyle çözümü sıfırdan başlatmak zorunda kalmasını ifade eder. Sık sık resetleme olması, özellikle yüksek doğruluklu PPP ya da RTK gibi uygulamalarda konum hesaplamasını büyük ölçüde etkiler.

12:15–12:45 arasında, GNSS alıcısının güvenilirliği ciddi şekilde zedelenmiştir. Sinyal kararlılığı bozulmuş, ambiguity çözümleme sıklıkla sıfırlanmış ve uydu sayısı güvenilir çözüm için kritik eşiğin altına düşmüştür.Bu durum, deneysel olarak jamming ya da spoofing saldırısının uygulandığı zaman dilimiyle çakışmakta, sinyal güvenliğini tehdit eden dış etkenlerin mevcudiyetini doğrulamaktadır.

5.2.9. Statik taşıyıcı faz artıkları (Carrier-phase residuals) zaman serisi analizi



Şekil 5.22. Statik taşıyıcı faz artıkları zaman serisi analizi

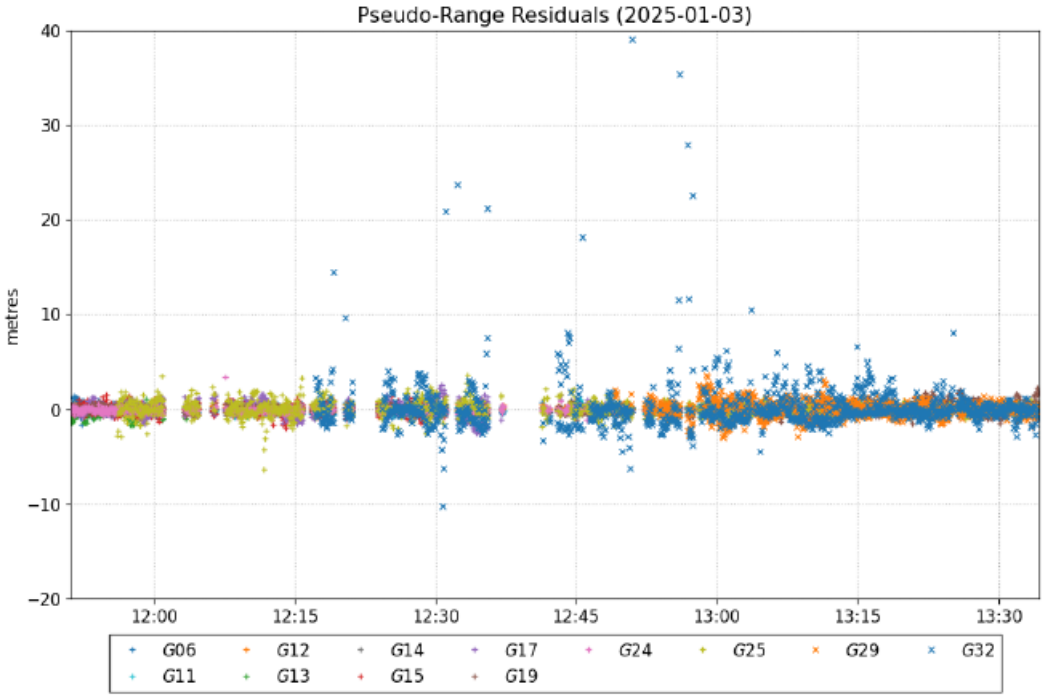
Taşıyıcı faz artık değerleri çoğunlukla ±0.01 metre sınırları içinde kalmakta olup bu, yüksek doğruluklu konumlandırma için oldukça iyi bir göstergedir.

12:25–12:45 aralığı: Bu zaman diliminde taşıyıcı faz artıklarında gözle görülür bir dağılma ve yayılma yaşanmıştır. Bazı artık değerler ±0.02–0.04 metreye kadar sapma göstermiştir.Özellikle bu aralıkta uydu G06 ve G32 gibi bazı uyduların artık değerlerinde ani sıçramalar dikkat çekmektedir. Bu durum, sinyalin doğru işlenemediğini ve modelin çözümleme sürecinde zorlandığını göstermektedir.

Faz artıklarındaki anormal dağılmalar, genellikle sinyal kalitesinde yaşanan bozulmaların yani jamming ya da spoofing bir sonucudur.

Eğer sistem istikrarlı bir ortamda çalışsaydı, bu artıklar zamana göre daha sabit ve sıkı bir aralıkta olmalıydı. Fakat 12:25–12:45 aralığında faz artıklarının ani ve düzensiz şekilde yükselmesi, taşıyıcı faz çözümlemesinin güvenilirliğini düşürmüş ve çözüm kalitesini olumsuz etkilemiştir.Bu da, GNSS sistemine yapılan bir sinyal müdahalesinin (jamming veya spoofing) göstergesi olarak yorumlanabilir.

5.2.10. Statik sahte menzil artıkları (Pseudo-range residuals) analizi



Şekil 5.23. Statik sahte menzil artıkları analizi

12:00 öncesinde ve 12:15–12:25 sonrası dönemde pseudo-range artık değerleri çoğunlukla ±2 metre aralığında kalmaktadır. Bu da GNSS kod çözümlemesinin büyük oranda sağlıklı işlediğini gösterir.

12:25–12:50 arası: Bu aralıkta ciddi bir bozulma görülmektedir. Artık değerler bazı uydularda 10, hatta 30–40 metre seviyelerine kadar sapmıştır. Bu, oldukça anormal ve ciddi bir hata büyüklüğüdür.

En çok sapma gösteren uydular arasında G06 ve G32 öne çıkmaktadır. Bu uydulara ait sinyallerin güvenilirliği bu aralıkta düşmüştür.

Bu derece yüksek artık değerleri, GNSS sinyaline müdahale olasılığını çok güçlü biçimde işaret eder. Çünkü; jamming durumunda sinyal gücü düşer ve çok yol etkisi oluşur.Spoofing durumunda ise alıcı sahte sinyalleri doğru zannederek konum hatasına düşer.

Özellikle 12:25–12:50 arasında oluşan bu ciddi sapmalar, jamming veya spoofing gibi bir tehdit altında GNSS alıcısının hatalı ölçüm yaptığına işaret etmektedir.

Kod ölçümlerindeki artık değerlerin aşırı büyümesi, sistemin doğruluk ve güvenilirliğini ciddi şekilde zayıflatır.Bu durum, taşıyıcı faz analizleriyle birlikte değerlendirildiğinde, o zaman aralığında GNSS sinyallerinin bozulduğunu veya yanıltıldığını açıkça göstermektedir.

5.2.11. Statik faz belirsizliği durumu analizi

Şekil 5.24. Statik Faz belirsizliği durumu analizi

- Yeşil (Fixed ambiguity): Faz belirsizliği sabitlenmiş, yüksek doğrulukta çözüm elde edilmiştir.
- Sarı (Float ambiguity): Faz belirsizliği henüz çözülmemiştir; konum doğruluğu nispeten daha düşüktür.
- Mavi (Datum ambiguity): Referans noktasına göre çözülmemiş belirsizliği gösterir.
- Kırmızı çizgiler (New arc): Sinyal kopması sonrası faz çözümlemesinin yeniden başlatıldığı noktaları gösterir.

12:00–12:45 arası çok sayıda uyduda sık sık *"new arc" (kırmızı çizgi)* oluşmuş ve float ambiguity (sarı) gözlemlenmiştir.Bu durum, sinyal bütünlüğünde bozulma olduğunu ve taşıyıcı faz çözümlemesinin bu aralıkta sağlıklı yapılamadığını göstermektedir.Özellikle G25, G32, G12 ve G24 uydularında sıklıkla float/yeniden başlama durumu yaşanmıştır.

12:45 sonrası birçok uyduda fixed ambiguity (yeşil) stabil şekilde sağlanmış ve sinyal kalitesi artmıştır.Bu da GNSS alıcısının yeniden güvenilir sinyal alımına geçtiğini ve çözümlemenin düzeldiğini gösterir.

Sık sık yeni arc oluşumu, sinyalin kesildiğini veya alıcının taşıyıcı faz çözümlemesini sıfırlamak zorunda kaldığını gösterir. Bu, jamming (karıştırma) etkisinin güçlü bir belirtisidir.Uzun süreli float ambiguity durumları, GNSS alıcısının sinyali çözümlerken kararsız kaldığını gösterir. Bu da spoofing (aldatma) etkisinin olabileceğini düşündürür.G11, G12, G25, G32 gibi uydularda belirgin faz çözümleme bozulmaları görülmüştür.

12:00–12:45 zaman aralığında GNSS sisteminde yüksek belirsizlik, faz çözümlemesinde kopmalar ve doğruluk kaybı yaşanmıştır.Bu da deneysel ortamda jamming/spoofing uygulamasının etkili olduğunu ve alıcının bu süreçte sinyalleri ya kaybettiğini ya da karıştırdığını açık biçimde ortaya koymaktadır.

6. SONUÇ VE ÖNERİLER

Bu tez çalışmasında, GNSS sistemlerinin jamming (karıştırma) ve spoofing (aldatma) saldırılarına karşı duyarlılığı deneysel olarak incelenmiş; hem kinematik hem de statik ölçüm koşullarında sinyal kalitesindeki bozulmaların konum doğruluğu üzerindeki etkileri detaylı şekilde değerlendirilmiştir. Gerçekleştirilen ölçümler sonucunda elde edilen veriler doğrultusunda, saldırı türlerinin GNSS konumlama sisteminde yarattığı hatalar nicel ve grafiksel olarak analiz edilmiştir.

Kinematik ve statik uydu gökyüzü dağılımı grafiğine bakıldığında uydu dağılımı dengelidir. Ancak belirsizlik oranı yaklaşık %45 oranındadır. Bu durum jamming ve spoofing uygulama etkilerini göstermektedir. Buna göre bazı uydular sinyal kaybına uğramış ve istenilen veriler elde edilememiştir.

Kinematik konum sapması dağılımı grafiğinde kümelerin yatay eksendeki dağılımı yaklaşık 0.4 m ile 1.0 m aralığındadır. Dikey eksendeki fark ise -2.6 m ile -3.0 m arasında değişmektedir. Bu, GNSS alıcısının saldırı öncesi ve sonrası konum çözümünün belirgin şekilde değiştiğini, yani sinyal güvenilirliğinin bozulduğunu göstermektedir.

Kinematik elipsoidal yükseklik zaman serisi grafiğine bakıldığında ise ilk başta yükseklik değerleri 670.8 – 671.1 m aralığında sabit kalmıştır. Bu, GNSS çözümünün istikrarlı olduğunu, uydu görünürlüğünün yeterli ve sinyal kalitesinin iyi olduğunu gösterir. Ancak jamming ve spoofing işlemleri uygulandıktan sonra bu değer yaklaşık 3 metreye kadar yükselmiş ve 674.3 m civarına ulaşmıştır. Bu sıçrama, GNSS çözümünün geçici olarak bozulduğunu ve sistemin yanlış yükseklik üretmeye başladığını gösterir.

Kinematik ve statik enlem farkı ve sigma (çözüm belirsizliği) zaman serisi grafiğinde ilkin enlem farkları genellikle -2.6 m ile -3.0 m arasında sabit kalmıştır bu dönem boyunca SIG_PPP değeri ise 0.1 m ile 0.3 m aralığındadır. Ancak karıştırma uygulaması sonrası enlem farkı yaklaşık -2.2 m'ye kadar yükselmiş, SIG_PPP değeri ise 3.5 metreyi aşmıştır. Bu ani sapma değeri karıştırma saldırısının etkisini göstermektedir.

Kinematik ve statik boylam farkı ve çözüm belirsizliği zaman serisi grafiğine bakıldığında boylam farkı yaklaşık 0.35 – 0.85 metre arasında sigma değerleri yaklaşık 0.1 – 0.3 m arasındadır. Uygulama sonrası boylam farkı 1.15 metreye kadar ulaşırken, sigma değeri 5 metreye kadar yükselmektedir.Bu durum spoofing etkisini göstermektedir.

Kinematik ve statik yükseklik farkı ve çözüm belirsizliği zaman serisi grafiğine göre yükseklik farkı yaklaşık 6.0 – 6.3 metre arasında iken SIG_PPP değeri de 0.1 – 0.3 metre seviyesindedir. Uygulamadan sonra bu değer yükseklik farkı yaklaşık 3 metrelik bir sapma ile 9.1 metreye kadar çıkmaktadır. Sigma değeri 21 metreyi aşmıştır. Bu ani artışlar, GNSS sisteminin konum çözümünde çözüm doğruluğunun neredeyse kullanılamaz hale geldiğini göstermektedir.

Kinematik ve statik troposferik zenit gecikmesi zaman serisi grafiğinde GNSS sinyallerinin atmosferik etkilerden büyük ölçüde bağımsız çalıştığını ve gözlenen konum sapmalarının meteorolojik değil spoofing veya jamming gibi dış kaynaklı nedenler olduğunu desteklemektedir.

Kinematik ve statik GNSS alıcı saat sapması zaman serisi grafiğinde sigma değeri 0 ns – 5 ns iken karıştırma işlemi sonrası bu değer 50 ns'ye kadar yükselmiştir. Bu karıştırma etkisini göstermektedir.

Kinematik ve statik izlenen uydu sayısı ve faz belirsizliği sıfırlama oranına bakıldığında izlenen uydu sayısı genellikle 7 ila 9 arasında değişmekteyken faz belirsizliği sıfırlama oranı genellikle % 0'dır. Uygulama sonrası izlenen uydu sayısı 5'e kadar düşmüş ve faz belirsizliği sıfırlama oranı %60'a kadar çıkmıştır. Bu oran karıştırma etkisini göstermektedir.

Kinematik ve statik taşıyıcı faz artıkları zaman serisi grafiğine bakıldığında çoğu zaman diliminde taşıyıcı faz artıklarının dağılımı ± 0.01 m bandında kaldığı görülmektedir. Ancak uygulama sonrası bu değerin bazı uydular için ± 0.03 m'ye kadar değişmesi sinyallerin bazı bölümlerinde daha seyrek ve dağınık dağılımlar oluşması karıştırma etkisini göstermektedir.

Kinematik ve statik sahte menzil artıkları grafiğinde değerlerin genellikle ± 5 metre sınırları içinde kalması beklenir. Uygulama sonrası bazı uydulara ait artık değerleri 30–40 metreye kadar çıkmıştır (özellikle G06 ve G32). Sapmalar hem pozitif hem negatif yönde olması, sinyallerinin kararsızlık yaşaması açıkça karıştırma ve yanıltma saldırılarının göstergesidir.

Kinematik ve statik faz belirsizliği durumu grafiğine bakıldığında uygulamadan önce uyduların çoğunda faz çözümünün tam olarak sabitlenemediğini, ancak izlenebilir ölçümler sağlandığını gösterir. Ancak uygulama sonrası birçok uyduda art arda yeni yaylar oluştuğu gözlemlenmektedir. Bu durum, jamming ve spoofing etkisiyle taşıyıcı faz sinyallerinin kararsız hale geldiğini ve çözüm sürecinin kesintiye uğradığını göstermektedir. Örneğin G32, G29, G25 gibi uydular bu aralıkta faz çözümüne yeniden başlamak zorunda kalmış ve sıklıkla yeni yaylar oluşturmuştur.

Sonuç olarak, GNSS sistemlerinin, çevresel sinyal bozucu etkilere karşı belirli düzeyde savunmasız olduğu bir kez daha deneysel olarak kanıtlanmıştır. GNSS sinyallerinin zayıf yapısı nedeniyle kolayca bastırılabilmesi ya da taklit edilmesi; özellikle savunma, ulaşım, tarım, sivil havacılık gibi hassas uygulamalarda ciddi güvenlik riskleri doğurmaktadır.

Daha sonraki çalışmalarda GNSS sinyallerinin güvenilirliği, çoklu GNSS sistemlerinin birlikte kullanılmasıyla artırılabilir; böylece tek bir sistemin hedef alınması durumunda sistem genel olarak daha dirençli hale getirilebilir. Anten ve alıcı donanımları, frekans seçicilik ve sinyal filtreleme açısından geliştirilerek jamming saldırılarına karşı daha dayanıklı hale getirilebilir. Yapay zeka destekli savunma sistemleri geliştirilerek, spoofing saldırılarına karşı sinyalin geldiği yön, sinyal gücü kontrol edilebilir.

Bu çalışma, özellikle konumsal güvenliğin kritik öneme sahip olduğu alanlarda, sinyal bozucu tehditlerin anlaşılması ve önlenmesine yönelik akademik ve pratik katkılar sağlamaktadır. Gelecek çalışmaların, sinyal bozucu etkileri erken tespit eden, sınıflandıran ve etkisizleştiren hibrit savunma sistemleri geliştirmeye odaklanması önerilmektedir.

KAYNAKÇA

Akos, D. M. (2012). Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *NAVIGATION: Journal of the Institute of Navigation*, *59*(4), 281-290.

Al-Soufi, L., Demirsoy, T., & Soyak, E. G. (2022). An Implementation-Based Study of the Detection of and Recovery from GPS Spoofing Attacks for Unmanned Aerial Vehicles. *International Journal of Advances in Engineering and Pure Sciences*, *36*(3), 211-223.

Analog Devices. (2020). ADALM-PLUTO User Guide. Retrieved from: https://wiki.analog.com/university/tools/pluto/users

Augustin, A., Yi, J., Clausen, T., & Townsley, W. M. (2016). A study of LoRa: Long range & low power networks for the internet of things. *Sensors*, *16*(9), 1466.

Burbank, J., Greene, T., & Kaabouch, N. (2024). Detecting and mitigating attacks on GPS devices. *Sensors*, *24*(17), 5529.

Bhatti, J., & Humphreys, T. E. (2017). Hostile control of ships via false GPS signals: Demonstration and detection. *NAVIGATION: Journal of the Institute of Navigation*, *64*(1), 51-66.

Chen, X., Dovis, F., Peng, S., & Morton, Y. (2013). Comparative studies of GPS multipath mitigation methods performance. *IEEE Transactions on Aerospace and Electronic Systems*, *49*(3), 1555-1568.

Dovis, F. (Ed.). (2015). *GNSS interference threats and countermeasures*. Artech House.

Egea-Roca, D., Arizabaleta-Diez, M., Pany, T., Antreich, F., Lopez-Salcedo, J. A., Paonni, M., & Seco-Granados, G. (2022). GNSS user technology: State-of-the-art and future trends. *IEEE Access*, *10*, 39939-39968.

Eurocontrol. (2021). EGNOS Service Definition Document. https://egnos-user-support.essp-sas.eu

Fu, Z., Wang, N., Shen, X., & Li, A. (2025). Temporal and Spatial Analysis of the Impact of the 2015 St. Patrick's Day Geomagnetic Storm on Ionospheric TEC Gradients and GNSS Positioning in China Using GIX and ROTI Indices. *Remote Sensing*, *17*(12), 2027.

Gao, G. X. GNSS Jammingin the Name of privacy.

GNU Radio Foundation. (2023). GNU Radio Documentation. https://wiki.gnuradio.org

Great Scott Gadgets. (2023). HackRF One Technical Overview. https://greatscottgadgets.com/hackrf/

Groves, P. D. (2014). The complexity problem in future multisensor navigation and positioning systems: A modular solution. *The Journal of Navigation*, *67*(2), 311-326.

Guo, J., Li, X., Li, Z., Hu, L., Yang, G., Zhao, C., ... & Ge, M. (2018). Multi-GNSS precise point positioning for precision agriculture. *Precision agriculture*, *19*, 895-911.

Han, C., Song, C., Wang, D., Guo, Y., Zhen, W., Bai, P., ... & Ruimin, J. Crowdsourced Smartphone-Based Machine Learning for Gnss Jammer Detection and Localization. *Available at SSRN 5119211*.

Hofmann-Wellenhof, B., Lichtenegger, H., & Wasle, E. (2007). *GNSS–global navigation satellite systems: GPS, GLONASS, Galileo, and more*. Springer Science & Business Media.

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (2008, September). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Proceedings of the 21st International technical meeting of the satellite division of the institute of navigation (ION GNSS 2008)* (pp. 2314-2325).

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, *2012*(1), 127072.

Janos, D., & Kuras, P. (2021). Evaluation of low-cost GNSS receiver under demanding conditions in RTK network mode. *Sensors*, *21*(16), 5552.

Kaplan, E. D., & Hegarty, C. (Eds.). (2017). *Understanding GPS/GNSS: principles and applications*. Artech house.

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of field robotics*, *31*(4), 617-636.

Khawaja, W., Ezuma, M., Semkin, V., Erden, F., Ozdemir, O., & Guvenc, I. (2022). A Survey on Detection, Tracking, and Classification of Aerial Threats using Radars and Communications Systems. *arXiv preprint arXiv:2211.10038*.

Koca, B., & Ceylan, A. (2018). *Uydu konum belirleme sistemlerindeki (GNSS) güncel durum ve son gelişmeler. Geomatik, 3 (1), 63-73*.

Leick, A., Rapoport, L., & Tatarnikov, D. (2015). *GPS satellite surveying*. John Wiley & Sons.

Li, X., Chen, L., Lu, Z., Wang, F., Liu, W., Xiao, W., & Liu, P. (2023). Overview of jamming technology for satellite navigation. *Machines*, *11*(7), 768.

Liu, Y., Li, S., Fu, Q., & Liu, Z. (2018). Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system. *Sensors*, *18*(5), 1433.

Lo, S. C., & Enge, P. K. (2010, May). Authenticating aviation augmentation system broadcasts. In *IEEE/ION position, location and navigation symposium* (pp. 708-717). IEEE.

Magiera, R., & Katulski, R. J. (2015). Detection and mitigation of GNSS spoofing based on antenna array processing. *Journal of Applied Research and Technology*, 13(1), 45–57.

Magiera, J., & Katulski, R. J. (2016). Performance evaluation of GPS anti-spoofing system based on antenna array processing. In *The European Navigation Conference-Enc*.

Misra, P., & Enge, P. (2006). *Global Positioning System: Signals, Measurements, and Performance.*

Misra, P., & Enge, P. (2011). Global positioning system: signals measurements.

Mitola, J. (1995). The software radio architecture. *IEEE Communications magazine*, *33*(5), 26-38.

NovAtel. (2021). What are Global Navigation Satellite Systems? (https://novatel.com/tech- talk/an-introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss#:~:text=A%20global%20navigation%20satellite%20system,for%20navigation%20and%20positioning%20measurements.)

Pavlovčič-Prešeren, P., Dimc, F., & Bažec, M. (2021). A comparative analysis of the response of GNSS receivers under vertical and horizontal L1/E1 chirp jamming. *Sensors*, *21*(4), 1446.

Pica, E., Minetto, A., Cesaroni, C., & Dovis, F. (2022). Unclassified Radio Frequency Interferer Affecting Ionospheric Scintillations Monitoring over the Mediterranean Area. *Authorea Preprints*.

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, *104*(6), 1258-1270.

Radoš, K., Brkić, M., & Begušić, D. (2024). Recent advances on jamming and spoofing detection in GNSS. *Sensors*, *24*(13), 4210.

Romaniuc, A. G., Vasile, V. C., & Borda, M. E. (2025). Global Navigation Satellite System Spoofing Attack Detection Using Receiver Independent Exchange Format Data and Long Short-Term Memory Algorithm. *Information*, *16*(6), 502.

Sanou, D. A. (2013). Analysis of GNSS interference impact on society and evaluation of spectrum protection strategies.

Schmidt, D., Radke, K., Camtepe, S., Foo, E., & Ren, M. (2016). A survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Computing Surveys (CSUR)*, *48*(4), 1-31

Schmidt, E., Ruble, Z., Akopian, D., & Pack, D. J. (2018). Software-defined radio GNSS instrumentation for spoofing mitigation: A review and a case study. *IEEE Transactions on Instrumentation and Measurement*, *68*(8), 2768-2784.

Songala, K. K., Ammana, S. R., Ramachandruni, H. C., & Achanta, D. S. (2020, December). Simplistic spoofing of GPS enabled smartphone. In *2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)* (pp. 460-463). IEEE.

Tanil, C., Jimenez, P. M., Raveloharison, M., Kujur, B., Khanafseh, S., & Pervan, B. (2018, September). Experimental validation of INS monitor against GNSS spoofing. In *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)* (pp. 2923-2937).

Teunissen, P. J., & Montenbruck, O. (Eds.). (2017). *Springer handbook of global navigation satellite systems* (Vol. 10, pp. 978-3). Cham, Switzerland: Springer International Publishing.

Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., & Capkun, S. (2011, October). On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security* (pp. 75-86).

Trimble Inc. (2021). *GNSS Surveying Systems Technical Guide*. Retrieved from https://www.trimble.com

U.S. Coast Guard. (2020). Differential GPS. https://www.navcen.uscg.gov/?pageName=dgpsMain

Van Diggelen, F. (2009). *A-gps: Assisted gps, gnss, and sbas*. Artech house.

Wanninger, L. (2004). Introduction to network RTK. *IAG Working Group*, *4*(1), 2003-2007.

Wang, F., Li, H., & Lu, M. (2017). GNSS spoofing detection and mitigation based on maximum likelihood estimation. *Sensors*, *17*(7), 1532.

Wang, W., Aguilar Sanchez, I., Caparra, G., McKeown, A., Whitworth, T., & Lohan, E. S. (2021). A survey of spoofer detection techniques via radio frequency fingerprinting with focus on the GNSS pre-correlation sampled data. *Sensors*, *21*(9), 3012.

Wu, Z., Zhang, Y., Yang, Y., Liang, C., & Liu, R. (2020). Spoofing and anti-spoofing technologies of global navigation satellite system: A survey. *IEEE Access*, *8*, 165444-165496.

Xue, Z., Lu, Z., Xiao, Z., Song, J., & Ni, S. (2022). Overview of multipath mitigation

technology in global navigation satellite system. *Frontiers in Physics*, *10*, 1071539.

Yang, Q., Zhang, Y., Tang, C., & Lian, J. (2019). A combined antijamming and antispoofing algorithm for GPS arrays. *International journal of Antennas and propagation*, *2019*(1), 8012569.

Yang, S., Khodabandeh, A., Zaminpardaz, S., & Teunissen, P. J. G. (2025). Ambiguity-resolved short-baseline positioning performance of LEO frequency-varying carrier phase signals: a feasibility study. *Journal of Geodesy*, *99*(2), 17.

Zumberge, J. F. (1997). Precise point positioning for the efficient and robust analysis of GPS data from large network. *J. Geophys. Res.*, *102*, 5-005.

ÖZGEÇMİŞ