KÜRESEL KONUMLANDIRMA SİSTEMİ (KKS) ALDATMA YÖNTEMLERİNİN VE KARŞI TEDBİRLERİN KARŞILAŞTIRILMASI

COMPARISON OF GLOBAL POSITIONING SYSTEM (GPS) SPOOFING METHODS AND COUNTERMEASURES

UMUT BERKAY DOKUMACI

DR. ÖĞR. ÜY. BARIŞ YÜKSEKKAYA

Tez Danışmanı

Hacettepe Üniversitesi

Lisansüstü Sınav Eğitim ve Öğretim Yönetmeliğinin

Elektrik-Elektronik Mühendisliği Anabilim Dalı için öngördüğü

YÜKSEK LİSANS TEZİ olarak hazırlanmıştır.

2024

ÖZET

KÜRESEL KONUMLANDIRMA SİSTEMİ (KKS) ALDATMA YÖNTEMLERİNİN VE KARŞI TEDBİRLERİN KARŞILAŞTIRILMASI

Umut Berkay DOKUMACI

YÜKSEK LİSANS TEZİ, Elektrik-Elektronik Mühendisliği

Danışman: Dr. Öğr. Üy. Barış YÜKSEKKAYA

2024, 149 sayfa

Küresel Konumlandırma Sistemi (Global Positioning System, GPS), dünya genelinde kritik öneme sahip bir teknoloji olup, konum belirleme, navigasyon ve zamanlama gibi çeşitli uygulamalarda kullanılmaktadır. Ancak, GPS sinyallerinin düşük güçlü yapısı nedeniyle, bu sinyallerin karıştırılması veya aldatılması mümkündür. Bu tezde, GPS aldatma saldırıları ve bu saldırılara karşı geliştirilen karşı tedbir yöntemleri detaylı bir şekilde incelenmiştir. Çalışmada, yeniden oynatma ve sahtecilik gibi aldatma stratejileri ile bu stratejilere karşı geliştirilen çeşitli karşı tedbir teknikleri deneysel olarak test edilmiştir. Yazılım Tabanlı Radyo (Software Defined Radio, SDR) kullanılarak gerçekleştirilen deneyler sonucunda, çeşitli GPS alıcılarının aldatılabilirliği gösterilmiş ve etkin karşı tedbir stratejileri belirlenmiştir. Elde edilen sonuçlar, GPS aldatma saldırılarına karşı hangi tekniklerin en etkili olduğunu ortaya koymakta ve gelecekteki çalışmalar için önemli bilgiler sunmaktadır.

Anahtar Sözcükler: Küresel Konumlandırma Sistemi (KKS), GNSS, GPS, Aldatma Saldırıları, Karşı Tedbirler, Yazılım Tanımlı Radyo (SDR), USRP, Konumlandırma Güvenliği, Sinyal Sahteciliği, Yeniden Oynatma Saldırıları

ABSTRACT

COMPARISON OF GLOBAL POSITIONING SYSTEM (GPS) SPOOFING METHODS AND COUNTERMEASURES

Umut Berkay DOKUMACI

Master of Science, Department of Electrical and Electronics Engineering

Supervisor: Asst.Prof. Barış YÜKSEKKAYA

June 2024, 149 page

The Global Positioning System (GPS) is a technology of critical importance worldwide, used in various applications such as positioning, navigation, and timing. However, due to the low power nature of GPS signals, these signals can be jammed or spoofed. This thesis provides a detailed examination of GPS spoofing attacks and the countermeasure methods developed to combat these attacks. The study experimentally tests various countermeasure techniques against spoofing strategies such as replay and forgery. Experiments conducted using the Software Defined Radio (SDR) demonstrated the susceptibility of various GPS receivers to spoofing and identified effective countermeasure strategies. The results obtained reveal which techniques are most effective against GPS spoofing attacks and offer valuable insights for future research.

Keywords: Global Positioning System (GPS), GNSS, GPS, Spoofing Attacks, Countermeasures, Software-Defined Radio (SDR), USRP, Positioning Security, Signal Falsification, Replay Attacks

TEŞEKKÜR

Bu tez çalışması boyunca benimle değerli bilgilerini ve desteğini paylaşan tez danışmanım Dr. Oğr. Üy. Barış YÜKSEKKAYA hocama, eğitim hayatım boyunca hep yanımda olan sevgi ve desteklerini esirgemeyen değerli aileme, başından sonuna kadar yanımda olan bu süreci benimle yaşayan hayat arkadaşıma, bu süreçte beni destekleyen şirketime ve ekip arkadaşlarıma ayrı ayrı çok teşekkür ederim.

İçindekiler

Sayfa

TABLOLAR

Sayfa

ŞEKİLLER

Sayfa

KISALTMALAR

A-GNSS : **A**ssisted **G**lobal **N**avigation **S**atellite **S**ystem
Yardımlı Küresel Konumlandırma Uydu Sistemi

Beidou : **B**ei **D**ou **N**avigation **S**atellite **S**ystem
Beidou Navigasyon Uydu Sistemi

CNR : **C**arrier-to-**N**oise **R**atio
Taşıyıcı-Gürültü Oranı

GNSS : **G**lobal **N**avigation **S**atellite **S**ystem
Küresel Konumlandırma Uydu Sistemi

GLONASS : **GL**Obal **N**Avigation **S**atellite **S**ystem
Küresel Uydu Navigasyon Sistemi

GPS : **G**lobal **P**ositioning **S**ystem
Küresel Konumlandırma Sistemi

IMU : **I**nertial **M**easurement **U**nit
Atalet Ölçüm Birimi

RAIM : **R**eceiver **A**utonomous **I**ntegrity **M**onitoring
Alıcı Bağımsız Bütünlük İzleme

SCER : **S**ecurity **C**ode **E**stimation and **R**eplay
Güvenlik Kodu Tahmini ve Yeniden Oynatma

sVid : **S**pace **V**ehicle **ID**entification
Uzay Aracı Kimlik Kodu

USRP : **U**niversal **S**oftware **R**adio **P**eripheral
Evrensel Yazılım Tanımlı Radyo Çevre Birimi

1 GİRİŞ

Küresel Seyrüsefer Uydu Sistemleri (Global Navigation Satellite System, GNSS), dünya genelinde bir dizi uydu sistemi kullanarak konumlandırma sağlayan kritik bir teknolojidir. Dünya üzerinde en yaygın şekilde kullanılan GNSS sistemi, Amerika Birleşik Devletleri (ABD) tarafından geliştirilen Küresel Konumlandırma Sistemi (Global Positioning System, GPS)'dir. GPS, 24 uydu tarafından sağlanan sürekli bir sinyal ağı aracılığıyla, kullanıcıların dünya üzerindeki herhangi bir noktadaki kesin konumlarını belirlemelerine olanak sağlar. GNSS, Rusya'nın GLONASS, Avrupa Birliği'nin Galileo ve Çin'in BeiDou gibi uydu konumlandırma sistemlerini de içermektedir.

Yüksek doğruluğu ve hassasiyeti ile GNSS, günlük yaşamda kullanılan pek çok uygulamada güvenilir konum bilgileri sağlamaktadır. Bu teknoloji, denizcilik ve havacılık sektörlerinde güvenli navigasyon ve uçuş, acil durum yönetiminde hızlı tepki verme, tarım sektöründe traktörlerin hassas konumlandırılması, iklim araştırmalarında atmosferdeki değişikliklerin izlenmesinden doğal afet tahminine kadar birçok uygulamada kullanılır. Ancak, bu teknolojinin birçok avantajı olmasına rağmen zayıflıkları da mevcuttur. GNSS sinyalleri çok uzak mesafelerden yayınlandıkları için alıcı tarafından alınan son derece zayıf sinyallerdir. Bu nedenle GNSS alıcılarının karıştırılması veya aldatılması nispeten kolaydır.

Son yıllarda geliştirilen Evrensel Yazılım Tanımlı Radyo Birimi (Universal Software Radio Peripheral, USRP) cihazlarına erişimin kolaylaşması ile birlikte GPS karıştırma veya aldatma tehditlerinin gerçekleşmesi de basitleşmiştir. Aldatma, GNSS alıcılarını yanlış yönlendirerek hatalı navigasyon çözümleri üretmeyi amaçlayan kasıtlı bir saldırıdır. Hedef alıcının bir saldırı yaşandığını tespit edememesi ve kullanıcıyı navigasyon çözümünün güvenilmez olduğu yönünde uyaramaması sebebiyle aldatma saldırıları karıştırma saldırılarından daha tehlikelidir.

Bu çalışmada, GPS aldatma saldırıları ve bu saldırılara karşı geliştirilen karşı tedbir yöntemleri detaylı bir şekilde incelenmiştir. Çalışma kapsamında, hem literatürde mevcut olan yöntemler detaylı bir şekilde incelenmiş hem de çeşitli deney ve simülasyonlarla

bu yöntemlerin etkinliği test edilmiştir. Yazılım Tabanlı Radyo (Software Defined Radio, SDR) kullanılarak doğal GNSS sinyalleri elde edilmiş ve açık kaynaklı GPS-SDR-SIM kütüphanesi kullanılarak GPS sinyalleri üretilmiştir. GPS aldatmasında temel stratejiler olan yeniden oynatma ve sahtecilik aldatma saldırıları detaylı bir şekilde incelenmiştir. Bu iki saldırı stratejisi, farklı alt kategorilerde ele alınmıştır. Gerçekleştirilen deneyler sonucunda, UBLOX M8N GNSS alıcısının, çeşitli cep telefonlarının ve farklı modeldeki İHA (İnsansız Hava Aracı)'ların aldatılabilirliği gösterilmiştir. USRP yardımıyla bazı aldatma yöntemleri uygulanmış ve cep telefonu, UBLOX alıcısı ve İHA gibi GNSS alıcılarının aldatılması başarılmıştır. Aynı zamanda belirtilen aldatma saldırıları altında karşı tedbir sağlanabilmesi için kullanılabilecek veriler kaydedilmiştir. Bu verilerden faydalınarak, CNR kontrollü karşı tedbir, sVid kontrollü karşı tedbir ve Doppler kaymasına göre karşı tedbir teknikleri incelenmiştir.

Elde edilen sonuçlar, GPS aldatma saldırılarına karşı en etkili savunma stratejilerinin belirlenmesine yardımcı olmuştur. Gerçekleştirilen deneylerde, çeşitli aldatma ve karşı tedbir yöntemlerinin performans analizleri yapılmıştır. Bu çalışmada mevcut literatürdeki bulguların gerçek bir sistemde birleştirilerek güvenlik açıklarının incelenmesi amaçlanmıştır. GPS aldatma ve karşı tedbir yöntemlerinin performans analizleri ile birlikte sunulan sonuçlar, GPS aldatma saldırılarına karşı hangi tekniklerin en etkili olduğunu ortaya koymak için kullanılmıştır. Bu değerlendirmeler, gerçekleştirilen GPS aldatma ve karşı tedbir yöntemlerinin etkinliğini ve uygulanabilirliğini ortaya koymaktadır.

Bu tezde sunulan sonuçlar, GPS aldatma saldırılarına karşı alınabilecek önlemler konusunda önemli bilgiler sağlamaktadır. Ancak, GPS teknolojisinin sürekli gelişen yapısı ve aldatma tekniklerinin çeşitliliği göz önüne alındığında, gelecekte daha kapsamlı çalışmalar yapılması gerekmektedir. Gelecekteki çalışmalar, daha gelişmiş aldatma tekniklerinin incelenmesi, yeni karşı tedbir yöntemlerinin geliştirilmesi ve bu yöntemlerin farklı GNSS alıcıları üzerinde test edilmesini içerebilir. Ayrıca, bu çalışmaların sonuçlarının, GPS aldatma saldırılarına karşı daha güçlü ve etkili savunma stratejilerinin oluşturulmasına katkıda bulunması beklenmektedir.

1.1 Tezin Katkıları

Bu tez çalışması, GPS aldatma ve karşı tedbir yöntemlerinin literatürdeki mevcut bilgileri detaylı bir şekilde inceleyerek ve bu yöntemlerin gerçek sistemler üzerinde test edilerek değerlendirilmesini sağlamaktadır. Çalışmanın önemli katkıları şunlardır:

- Literatürde belirtilen GPS aldatma yöntemleri ve karşı tedbirlerinin karşılaştırılması ve sınıflandırılması.
- USRP yardımıyla gerçeklenmiş GPS aldatma yöntemlerinin deneysel olarak test edilmesi.
- Cep telefonu, UBLOX alıcısı ve İHA gibi GNSS alıcılarının aldatılması ve bu aldatma yöntemlerine karşı geliştirilen karşı tedbirlerin etkinliğinin değerlendirilmesi.
- Elde edilen sonuçların performans analizleri ile birlikte sunulması ve en etkili karşı tedbir stratejilerinin belirlenmesi.

1.2 Organizasyon

Tez çalışmasının organizasyonu şu şekildedir:

- **Bölüm 1:** Giriş kısmı, çalışmanın amacını, kapsamını ve katkılarını açıklar.
- **Bölüm 2:** Küresel Uydu Seyrüsefer Sistemi ve Evrensel Yazılım Tanımlı Radyo Birimi hakkında temel bilgiler sunar.
- **Bölüm 3:** GPS aldatma yöntemleri ve bu saldırılara karşı geliştirilen karşı tedbirlerin çalışma mantıkları incelenerek literatür taraması yapılır.
- **Bölüm 4:** Gerçeklenmiş GPS aldatma ve karşı tedbir yöntemlerinin deneysel çalışmaları ve sonuçları sunulur.
- **Bölüm 5:** GPS aldatma ve karşı tedbir yöntemlerinin performans analizleri yapılır.

- **Bölüm 6:** Sonuçlar ve gelecekte yapılacak çalışmalar hakkında genel değerlendirmeler yapılır.

2 KÜRESEL SEYRÜSEFER UYDU SİSTEMİ VE EVRENSEL YAZILIM TANIMLI RADYO BİRİMİ

2.1 Küresel Uydu Seyrüsefer Sistemi

Küresel Seyrüsefer Uydu Sistemleri (Global Navigation Satellite System, GNSS) dünya üzerinde bulunan canlılar veya yapılar için konum ve zaman bilgisi sinyalleri yayan uydular sistemidir. Bu sistemlerin en yaygını olan Küresel Konumlandırma Sistemi (Global Positioning System, GPS) Amerika Birleşik Devletlerine ait olan uydular üzerinde kurulmuştur ve ABD tarafından işletilmektedir. GPS haricinde Glonass, Beidou, Galileo gibi uydu sistemleri de mevcuttur ve farklı ülkeler/birlikler tarafından işletilmektedir. Tablo 2.1'de GNSS Sistemlerinin karşılaştırılması verilmiştir. [5].

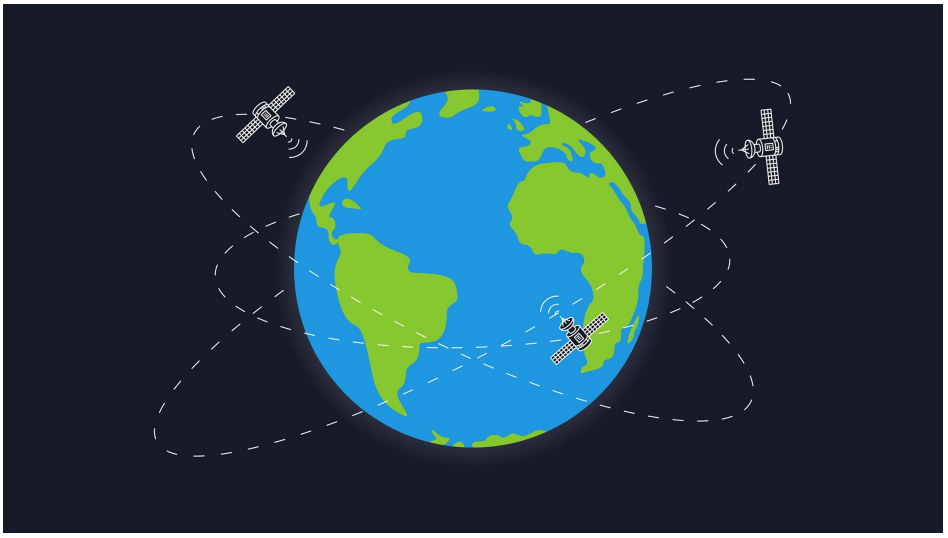
Küresel Navigasyon Uydu Sistemleri konum ve zaman bilgisine ulaşmayı sağladığı için çok yaygın kullanım alanına sahiptir. Özellikle havacılık, ulaşım ve tarım gibi sektörlerde bu teknoloji aktif olarak kullanılmakta ve geliştirilmeye devam etmektedir.

Tablo 2.1 GNSS Sistemlerinin Karşılaştırılması

Özellik	**GPS**	**GLONASS**	**BeiDou**	**Galileo**
Sahibi	Birleşik Devletler	Rusya	Çin	Avrupa Birliği
Sinyal Kodları	CDMA	FDMA	CDMA	CDMA
Yeryüzüne Yükseklik (İrtifa)	20.180 km	19.130 km	21.150 km	23.222 km
Yörünge Süresi	11,97 sa	11,26 sa	12,63 sa	14,08 sa
Devrimleri başına yıldızıl gün	2	17/8	17/9	17/10
Uydu Sayısı	31 (tasarımı ile en az 24)	28 (tasarımı ile en az 24 uydu)	5 jeosenkron yörünge, 30 orta yörünge	3 jeosenkron yörünge, 4 jeosenkron yörünge
Frekans	1,57542 GHz (L1), 1,2276 GHz (L2), 1,17645 GHz (L5)	Çevresi 1,602 GHz (SP), Çevresi 1.246 GHz (SP)	1,561098 GHz (B1), 1,589742 GHz (B1-2), 1,20714 GHz (B2), 1,26852 GHz (B3)	1,164–1,215 GHz (E5a ve E5b), 1,260–1.300 GHz (E6), 1,559–1,592 GHz (E2-L1-E11)
Durumu	İşletimde	İşletimde	15 uydu işletimde	Tam Operasyonel

2.2 Küresel Konumlandırma Sistemi

Küresel Konumlandırma Sistemi (Global Positioning System, GPS), tüm dünyada aktif olarak kullanılan uydu tabanlı bir konumlandırma sistemidir [6]. GPS projesi, öncelikle navigasyon sistemlerinin kısıtlı işlevselliğini aşabilmek amacıyla 1960'lardan gelen bir dizi gizli mühendislik çalışması da dahil olmak üzere, ilk denemelerde ortaya çıkan birkaç görüşün de bütünleştirilmesiyle 1973 yılında geliştirilmiştir [7]. GPS, ABD Savunma Bakanlığı (Department of Defense, DoD) tarafından esas olarak 24 uydu ile çalışacak şekilde tasarlanıp yapılmış ve devreye alınmıştır. 1994 yılında tam olarak işler hale gelmiştir. Sistem, Bradford Parkinson, Roger L. Easton ve Ivan A. Getting'in icatları ile güçlendirilmiştir [1].



Şekil 2.1 Küresel Konumlandırma Sistemi [1]

2.2.1 Geçmişten Günümüze GPS

GPS sistemi, ilk olarak askeri gereksinimler için tasarlanmıştır. Tasarımı, II. Dünya Savaşı sırasında kullanılan ve uzun süre hizmet veren Uzun Menzilli Navigasyon (Long Range Navigation, LORAN) ve Decca Navigasyon (Decca Navigator) gibi yer tabanlı radyo-seyir sistemlerine dayanmaktadır. GPS'in ilk kullanımı İkinci Dünya Savaşı'nın hemen sonrasına dayanmaktadır. Sistem, sinyal alıcıları ile yön bulma, askeri planlarda ve

konum hesaplamalarında, güdümlü roketlerin kontrolünde kullanılmak üzere tasarlanmıştır. Ancak GPS sistemi, sivil kullanıma 1980'lerde açılmıştır [1].

1956 yılında, Friedwardt Winterberg yapay uydular için genel görelilik denemesi önermiş ve bu da GPS'nin ilham kaynağı olmuştur. William Guier ve George Weiffenbach, Sputnik'in radyo sinyallerini izleyerek yörüngedeki konumunu belirlemeye karar vermişlerdir. Bu, Transit sisteminin geliştirilmesine yol açmıştır. 1960 yılında, Amerika Birleşik Devletleri Deniz Kuvvetleri tarafından kullanılan ilk uydu navigasyon sistemi olan Transit başarıyla test edilmiştir. 1967'de, ABD Deniz Kuvvetleri Timation uydusuyla yüksek doğruluklu saat ölçümü için uzay koşullarında yeteneklerini kanıtlamıştır. GPS'nin gelişimi, askeri ve sivil kullanım için kapsamlı bir ihtiyacın sonucu olarak görülmemiştir. Ancak Soğuk Savaş sırasında ABD'nin nükleer caydırıcılık politikası için gerekliliği ortaya çıkmış ve GPS'nin gizlice finanse edilmesine neden olmuştur. 1983'te, Kore Hava Yolları'na ait bir uçak Sovyetler Birliği'nin yasak hava sahasına girerek düşürülmüştür. Bu olay, GPS'in sivil kullanıma açılmasını hızlandırmıştır. 2000 yılında, Başkan Bill Clinton, GPS sinyallerinin hassaslığını iyileştirmek için seçici durumu kapatarak sivil kullanıcılara daha doğru konumlandırma sağlamıştır. ABD, GPS hizmetinde çeşitli iyileştirmeler yaparak sistemini geliştirmeye devam etmektedir. Bu, askeri, sivil ve ticari ihtiyaçları karşılamak ve sistemi yükseltmek için bir girişimdir. GPS, ABD Hükümeti'nin sahip olduğu ve işlettiği ulusal bir kaynaktır. Savunma Bakanlığı, GPS resmi temsilcisidir ve GPS politikalarını yönetmek için kurulmuş bir İcra Kurulu bulunmaktadır.

2.2.2 GPS'in Temelleri

GPS'in temel kullanım amacı, dünyanın herhangi bir noktasında bulunan bir nesnenin veya kişinin konumunu belirlemektir. GPS alıcısı, Dünya'nın yörüngesindeki GPS uydularından gönderilen hassas zamanlama sinyallerini kullanarak konumunu hesaplar. Her uydu sürekli olarak zaman bilgisini ve kendi konumunu içeren mesajları yayınlar. Alıcı, aldığı bu mesajların geçiş süresini belirleyerek ve ışık hızını kullanarak her bir uyduya olan mesafeyi hesaplar. Bu mesafeler ve uydu konumları, konumlama denklemleri kullanılarak alıcının

konumunu hesaplamak için kullanılır. Sonuç olarak, alıcının konumu belki de bir harita ekranında veya enlem ve boylam koordinatları olarak gösterilirken, yükseklik verisi jeoidin yukarıdaki yüksekliğine göre dâhil edilebilir. Bu şekilde, GPS alıcısı kullanıcıya konumunu hassas bir şekilde belirleme imkanı sağlar.

Temel GPS ölçümleri sadece bir konumun ne hız ne de yönünü verir. Ancak, çoğu GPS cihazıyla otomatik olarak iki veya daha fazla konumun ölçümleriyle konumun hızını ve hareket yönünü elde edilebilir. Bu ilkenin sakıncası, hız veya yön değişikliğinin yalnızca bir gecikmeyle hesaplanarak elde edilebilmesidir ve elde edilen yön uzaklığı ise iki konumun ölçümleri arasında seyahat ederken hatalı olmasıdır, altında veya yakınındaki konumun ölçümü rastgele hataya düşer. GPS cihazıyla doğru hızını hesaplamak için sinyallerin doppler kayması ölçümlerini kullanabilirsiniz.[8] Daha gelişmiş konumlandırma dizgeleri GPS'i tamamlayacak bir pusula ya da ataletsel konumlandırma sistemi gibi ek algılayıcılarda kullanır.

Temel bir GPS sinyal alımı işleminde, dört veya daha fazla uydu doğru bir sonuç elde etmek için görünür olmalıdır. Gezinme denklemlerin çözümü böylece daha doğru ve muhtemelen elverişsiz alıcı esaslı saat için ihtiyacı ortadan kaldırarak, alıcının yerleşik saat ve gerçek zaman günü tarafından tutulan saat arasındaki farkı ile birlikte alıcının konumu belirtir. Bu zaman aktarımı trafik sinyal zamanlaması ve cep telefonu baz istasyonları senkronizasyonu gibi GPS uygulamaları için bu ucuz ve son derece hassas zamanlamadan yararlanabilir.

Dört uydu normal çalışması için gerekli olmakla birlikte, daha azıda özel durumlarda geçerli olabilir. Bir değişkeni zaten biliniyorsa, bir alıcı ile sadece üç uydu kullanılarak konum belirlenebilir. Örneğin, bir gemi veya uçak yüksekliği bilinenlerden olabilir. Bazı GPS alıcıları bilinen son rakımın yeniden kullanılması gibi ilâve ipuçları ya da parekete hesabı, ataletsel konumlama, veya dâhili olarak ilâve ipuçları ya da varsayımlarını kullanabilir.

GPS'in temelde işleyişi üç ana bileşen üzerine kuruludur: uzay segmenti, kontrol segmenti ve kullanıcı segmenti.

Uzay Segmenti: Uydu grubunu içerir. GPS'te 24 veya daha fazla uydu, dünya yörüngesinde döner. Bu uydu grubu, dünya yüzeyinin çeşitli bölgelerinden her zaman görülebilen birkaç uydu içerir. Her uydu, dünyanın etrafında iki tam dönüş yaparak gün içinde iki kez bulunduğu konuma geri döner.

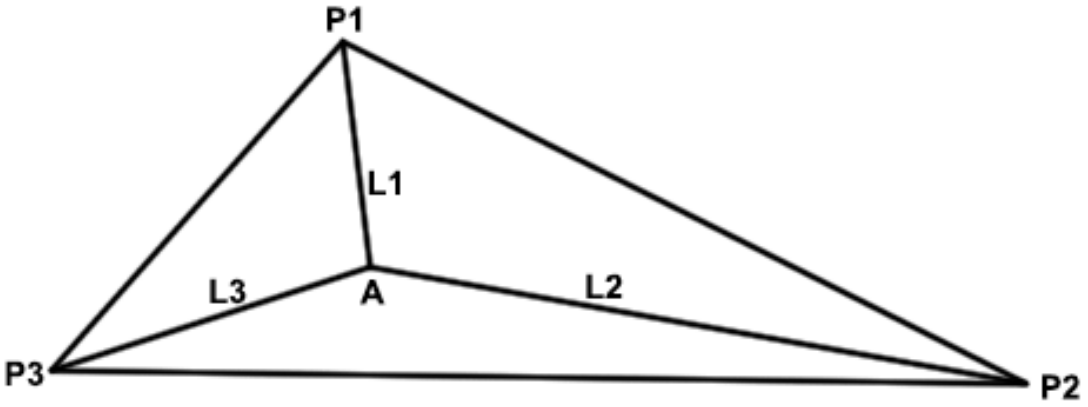
Kontrol Segmenti: GPS sinyallerini yöneten ve uydu hareketlerini izleyen bir ağdır. ABD Hava Kuvvetleri tarafından işletilen bir dizi izleme istasyonu ve kontrol merkezi bulunmaktadır. Bu istasyonlar, uydu sinyallerini izleyerek ve saatlerini senkronize ederek uydu pozisyonlarını doğrularlar.

Kullanıcı Segmenti: GPS alıcılarından oluşur. Kullanıcılar, GPS alıcılarını kullanarak uydu sinyallerini alır ve bunları işlerler. Alıcı, en az dört uydu sinyalini alarak, kendi konumunu hesaplamak için gereken bilgileri elde eder. Alıcı, gelen sinyallerin zaman farklarını ve uydu konumlarını kullanarak konumunu belirler.

GPS alıcıları, alınan sinyallerin zamanlamasını ve uydu pozisyonlarını kullanarak kullanıcının konumunu belirler. Bu süreç, zaman damgası bilgilerini ve uydu pozisyonlarını karşılaştırarak üç boyutlu bir konum tahmini yapar.

2.2.21. Üçgenleme GPS ve üçgenleme (trilateration), konum tespiti için mesafe ölçümlerine dayanan tekniklerdir. Ancak, GPS'te mesafeler, Dünya yüzeyindeki kontrol noktalarına değil, yaklaşık 20.183 km yükseklikte dönen uydulara göre ölçülür. GPS uyduları, bu yörüngelerde dönen kontrol noktalarıdır ve bilinmeyen bir noktada kesişen dört doğru vardır çünkü x (yükseklik), y (uzunluk), z (derinlik) ve zaman olmak üzere dört bilinmeyen çözülmesi gerekmektedir. Trilaterasyonda ise, en az üç kontrol istasyonu bulunur ve bu istasyonlardan üç kesişen mesafe elde edilir. Kontrol noktaları Dünya'nın yüzeyindedir ve mesafeler, elektronik olarak ışığın hızına ve sinyalin kontrol noktasından bilinmeyen noktaya ve bazı durumlarda geri gitmesi için geçen süreye bağlı olarak ölçülür. Her iki durumda da, mesafelerin doğru kontrol noktalarıyla eşleştirilmesi gerekir. GPS çözümü ile yersel ölçmenin bazı benzerlikleri vardır. Ancak, GPS'te mesafelerin elektronik

olarak ölçülmesi tek yönlüdür. Her iki durumda da, bilinmeyen bir noktanın konumunu bulmak için kullanılan mesafe kavramları, temel bir fikirdir.



Şekil 2.2 Üçgenleme

2.2.22. Soyut Mesafe GPS alıcısı ile GPS uydusu arasındaki ölçülen veya gözlemlenen mesafe, sinyalin uydudan alıcıya gelene kadar geçen süre olarak tanımlanır. Bu süre, ”sinyal seyahat süresi” olarak bilinir ve ışık hızıyla çarpılarak hesaplanır. Ancak, bu mesafe doğrudan ölçülen bir değer değildir, geometrik olarak ölçülmediği için ”pseudo” (sahte) olarak adlandırılır. Sinyal gecikmeleri veya alıcı kaynaklı hatalar gibi etkenler, psudorange hesaplamasını etkileyebilir. Alıcının kesin konumunu hesaplayabilmesi için birden çok uydu ve onların soyut mesafe (psudorange) verileri kullanılır. Bu verilerin doğru bir şekilde işlenmesi, GPS alıcısının doğru konumunu belirlemesini sağlar.

2.2.23. Soyut Rastgele Gürültü GPS’te her bir uydu, Soyut Rastgele Gürültü (Pseudo-Random Noise, PRN) adı verilen kendine özgü bir kod kullanır. Bu kodlar, önceden belirlenmiş rastgele ve benzersiz sayı dizinlerinden oluşur ve GNSS sinyalinin hangi uydunun ürettiğini belirtir. PRN kodları, bir uyduyu diğerlerinden ayırt etmek için kullanılır ve her bir uydunun belirli bir PRN kodu vardır. Bu kodlar, uydunun zaman dilimini ve pozisyonunu hesaplamak için alıcılar tarafından kullanılır. PRN kodları aynı zamanda konum tespiti ve zaman senkronizasyonu gibi işlemlerde de önemli bir rol

oynar. Bu kodlar, GPS sisteminin doğru ve güvenilir çalışmasını sağlamak için kritik bir öneme sahiptir.

2.2.24. Efemeris Efemeris bir GPS uydusunun belirli bir zamandaki tahmini konumunu, hızını ve saat bilgisini içeren verilerdir. Her GPS uydusu, alıcının doğru bir konum belirlemesi için gereken zaman, konum ve hız gibi bilgileri içeren bir efemeris verisi yayınlar. Efemeris verileri, uydu tarafından gönderilir ve GPS alıcıları tarafından alınarak kullanılır. Bu veriler, uydu tarafından gönderilen sinyaldeki saat bilgisine dayanarak uydu konumunu belirlemek için kullanılır. Matematiksel hesaplamalara dayanan bu veriler, alıcının konumunu doğru bir şekilde hesaplamak için gereklidir. Tipik olarak, GPS alıcıları günlük olarak birçok uydu iletişim kurar ve bu uydu verilerini alır. Bu efemeris verileri, alıcının mevcut konumu ve zamanı temel alarak uygun bir uydu seçmesine ve konumunu doğru bir şekilde hesaplamasına olanak tanır. Efemeris verileri, GPS sinyallerinin güvenilirliğini ve doğruluğunu sağlamak için kritik öneme sahiptir ve alıcıların doğru bir şekilde konum belirlemesine yardımcı olur. Şekil 2.3' de efemeris verisinin içeriğine ait bir örnek gösterilmiştir.

```
     2             NAVIGATION DATA                         RINEX VERSION / TYPE
CCRINEXN V1.6.0 UX  CDDIS               09-DEC-23 19:09     PGM / RUN BY / DATE
IGS BROADCAST EPHEMERIS FILE                                COMMENT
    0.2049D-07 -0.7451D-08 -0.5960D-07  0.1788D-06          ION ALPHA
    0.1372D+06 -0.1802D+06  0.6554D+05  0.6554D+05          ION BETA
    0.000000000000D+00-0.710542735760D-14   147456     2292 DELTA-UTC: A0,A1,T,W
    18                                                      LEAP SECONDS
                                                            END OF HEADER
 1 23 12  9  0  0  0.0 0.163725577295D-03 0.454747350886D-12 0.000000000000D+00
   0.800000000000D+01-0.797500000000D+02 0.387408994282D-08-0.559409706231D+00
  -0.412948429585D-05 0.130082704127D-01 0.742450356483D-05 0.515402762032D+04
   0.518400000000D+06-0.763684511185D-07-0.111214951251D+01 0.193715095520D-06
   0.990386838227D+00 0.251406250000D+03 0.999820641012D+00-0.800033324599D-08
  -0.290726395636D-09 0.100000000000D+01 0.229100000000D+04 0.000000000000D+00
   0.200000000000D+01 0.630000000000D+02 0.512227416039D-08 0.800000000000D+01
   0.516888000000D+06 0.400000000000D+01 0.000000000000D+00 0.000000000000D+00
 2 23 12  9  0  0  0.0-0.518206972629D-03 0.522959453519D-11 0.000000000000D+00
   0.430000000000D+02-0.935000000000D+02 0.430696511667D-08 0.206301044448D+01
  -0.492297112942D-05 0.162391446065D-01 0.593252480030D-05 0.515391137123D+04
   0.518400000000D+06 0.230967998505D-06-0.121510655774D+01-0.763684511185D-07
   0.967441954161D+00 0.261375000000D+03-0.129377965441D+01-0.785639867911D-08
  -0.407159816983D-09 0.100000000000D+01 0.229100000000D+04 0.000000000000D+00
   0.200000000000D+01 0.000000000000D+00-0.176951289177D-07 0.430000000000D+02
   0.513228000000D+06 0.400000000000D+01 0.000000000000D+00 0.000000000000D+00
 3 23 12  9  0  0  0.0 0.408878549933D-04 0.273985278909D-10 0.000000000000D+00
   0.960000000000D+02-0.100312500000D+02 0.389016204086D-08-0.166371948318D+01
  -0.553205609322D-06 0.505266687833D-02 0.995583832264D-05 0.515355508232D+04
   0.518400000000D+06 0.104308128357D-06-0.833540848779D-01 0.558793544769D-08
   0.982229115477D+00 0.200687500000D+03 0.110956567002D+01-0.763138930657D-08
   0.316084594764D-09 0.100000000000D+01 0.229100000000D+04 0.000000000000D+00
   0.200000000000D+01 0.000000000000D+00 0.186264514923D-08 0.960000000000D+02
   0.511218000000D+06 0.400000000000D+01 0.000000000000D+00 0.000000000000D+00
 4 23 12  9  0  0  0.0 0.234403181821D-03 0.101181285572D-10 0.000000000000D+00
   0.600000000000D+01-0.981250000000D+01 0.473555439771D-08 0.134679409545D+01
  -0.379979610443D-06 0.273843633477D-02 0.544637441635D-05 0.515359613991D+04
   0.518400000000D+06-0.149011611938D-07 0.996153114164D+00 0.372529029846D-07
   0.963597775567D+00 0.275812500000D+03-0.304623001987D+01-0.817355474708D-08
```

Şekil 2.3 Örnek Efemeris Verisi İçeriği

2.2.25. Almanak Almanak bir GPS alıcısının uydu konumlarını tahmin etmek için kullandığı veri setini ifade eder. Almanak verisi, GPS alıcısının birkaç gün ileriye veya geriye bakarak uydu konumlarını tahmin etmesine olanak tanır. Bu veri seti, GPS alıcısının hangi uydu sinyallerini arayacağını ve hangi uydu sinyallerini bekleyeceğini belirlemesine yardımcı olur.

Almanak verisi, uydu sinyallerini alıcının konumuna göre tahmin etmek için kullanılır. Her GPS uyduyu temsil eden almanak verisi, uyduyun tahmini konumu, yörünge bilgileri, saat düzeltmeleri ve diğer parametreleri içerir.

GPS alıcıları, almanak verisini alarak gelecekteki uydu konumlarını tahmin edebilir. Bu tahminler, alıcının konumunu ve zamanını dikkate alarak yapılır. Alıcılar, almanak verisini güncellemek için periyodik olarak GPS sinyalleri alır ve yeni almanak verisini alır.

Almanak verisi, GPS alıcılarının hızlı bir şekilde uydu sinyallerini bulmasına ve konum belirlemesine yardımcı olur. Ayrıca, almanak verisi alıcının bataryasını ve işlem gücünü korumak için daha az miktarda veri almasını sağlar, çünkü alıcı sadece gerekli olan uydu sinyallerini arar. Şekil 2.4' de almanak verisinin içeriğine ait bir örnek gösterilmiştir.

```
******** Week 261 almanac for PRN-02 ********
ID:                         02
Health:                     000
Eccentricity:               0.1604175568E-001
Time of Applicability(s):  319488.0000
Orbital Inclination(rad):   0.9676686368
Rate of Right Ascen(r/s):  -0.7908900866E-008
SQRT(A)  (m 1/2):           5153.661133
Right Ascen at Week(rad):   0.2814132322E+001
Argument of Perigee(rad):  -1.206617453
Mean Anom(rad):             0.2482581999E+001
Af0(s):                    -0.4558563232E-003
Af1(s/s):                   0.7275957614E-011
week:                        261

******** Week 261 almanac for PRN-03 ********
ID:                         03
Health:                     000
Eccentricity:               0.5310058594E-002
Time of Applicability(s):  319488.0000
Orbital Inclination(rad):   0.9837394824
Rate of Right Ascen(r/s):  -0.7486026109E-008
SQRT(A)  (m 1/2):           5153.705566
Right Ascen at Week(rad):  -0.2335839284E+001
Argument of Perigee(rad):   1.065678100
Mean Anom(rad):            -0.1039562601E+001
Af0(s):                     0.3032684326E-003
Af1(s/s):                   0.2182787284E-010
week:                        261
```

Şekil 2.4 Örnek Almanak Verisi İçeriği

2.2.26. Alıcı Bağımsız Bütünlük İzleme GPS sinyallerinde alıcı bağımsız bütünlük izleme (Receiver Autonomous Integrity Monitoring, RAIM) denilen bir yöntem kullanılır. Bu yöntem birden fazla uydudan alınan GPS sinyalinin doğrulunu teyitlemek amacıyla kullanılır.

2.2.27. Yardımlı Küresel Konumlandırma Uydu Sistemi Yardımlı Küresel Konumlandırma Uydu Sistemi (Asisted Global Navigation Satellite System, A-GNSS), geleneksel GNSS alıcılarının, örneğin GPS, GLONASS, Galileo ve BeiDou'nun performansını ve doğruluğunu artıran bir teknolojidir. A-GNSS, uydu sinyali alımını ve konumlandırmayı hızlandırmak ve doğruluğunu artırmak için harici kaynaklardan ek bilgileri kullanır.

A-GNSS genellikle, hücresel ağlar veya özel A-GNSS sunucuları gibi karasal kaynaklardan gelen verileri kullanarak GNSS alıcılarına yardımcı veri sağlar. Bu yardım verileri, uydu ephemeris verileri, almanak verileri, zaman bilgisi ve uydu sinyal gücü tahminleri gibi bilgileri içerir. Bu ek verileri kullanarak, A-GNSS alıcıları özellikle şehir içi kanyonlar veya kapalı mekanlar gibi uydu sinyallerinin zayıf veya engellenmiş olabileceği zorlu ortamlarda sinyal alımını daha hızlı gerçekleştirebilir.

A-GNSS'nin temel faydaları arasında daha hızlı ilk konum bulma süresi (time to first fix, TTFF), iyileştirilmiş konumlandırma doğruluğu ve özellikle zayıf uydu görünürlüğü olan ortamlarda daha iyi güvenilirlik bulunmaktadır. A-GNSS teknolojisi, akıllı telefonlardan otomobil navigasyon sistemlerine, giyilebilir cihazlara ve hassas konumlandırmanın önemli olduğu diğer uygulamalara geniş çapta kullanılmaktadır.

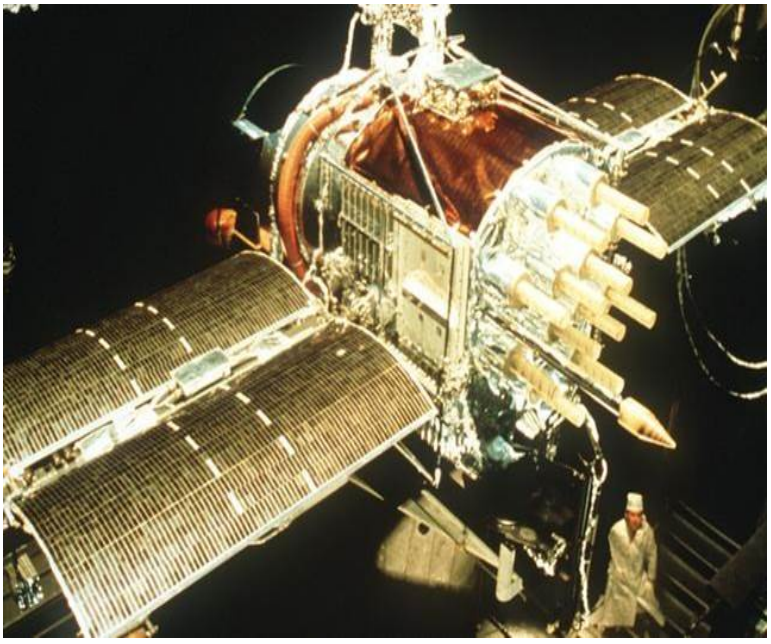
2.3 Küresel Konumlandırma Sistemi Modernizasyonu

GPS, sürekli olarak modernizasyon gerektiren kritik bir küresel hizmettir. Teknolojik gelişmelerin hızla ilerlemesiyle birlikte, GPS'in mevcut sistemleri önemli ölçüde geliştirilmiş ve güncellenmiştir. GPS Uzay Segmentinin konfigürasyonu, detaylı bir şekilde bilinmektedir. Uydular, Dünya'dan yaklaşık 20.000 km yükseklikte bir yörüngede

dolaşmaktadır. Bu sistemde üç taşıyıcı frekans bulunmaktadır: L1 (1575,42 MHz), L2 (1227,60 MHz) ve L5 (1176,42 MHz). En az 24 GPS uydusu dünya çapında 24 saatlik kapsama alanı sağlar, ancak yörüngede bu minimumdan daha fazlası mevcuttur. Ayrıca, uzayda birkaç yedek uydu da bulunmaktadır. GPS konumlandırma, navigasyon ve zamanlama gibi kritik hizmetlerin sağlanmasında önemli bir role sahiptir. Bu nedenle, yedekleme önlemi almak önemlidir, çünkü bu sistemlerin kesintisiz işleyişi modern yaşamın birçok alanı için gereklidir.

GPS, teknolojik zorluklar göz önüne alındığında hızlı bir şekilde uygulanmış ve 17 Temmuz 1995 tarihinde Tam Operasyonel Yeteneğe (Full Operational Capability, FOC) ulaşmıştır. Ancak, mevcut takımyıldızdaki en eski uydular 1990'ların sonlarında fırlatılmıştır. Bu nedenle, sistemi güncellemek ve iyileştirmek için planlar yapılmıştır. 2000 yılında ABD Kongresi, GPS III projesine yetki vermiştir. Bu proje, yeni yer istasyonları ve uydular, ek sivil ve askeri navigasyon sinyalleri ve daha iyi kullanılabilirlik gibi unsurları içermektedir.

2.3.1 Block I Uyduları



Şekil 2.5 Block I Uydusu 1978 – 1985 [2]

Block I Özellikleri:

- L1 (CA) seyir sinyali
- L1 & L2 (P Kodu) seyir sinyali
- 4.5 Yıl tasarım ömrü

Vandenberg Hava Kuvvetleri Üssü'nden 1978 ile 1985 yılları arasında fırlatılan 11 GPS uydusu, Blok I uyduları olarak bilinmektedir. Bu uyduların tamamı, GPS konumlandırma konseptini doğrulamak amacıyla inşa edilmiş prototip uydulardır ve Rockwell International tarafından üretilmiştir. Uyduların on tanesi Atlas F roketleriyle yörüngeye oturtulmuş, ancak bir fırlatma başarısızlıkla sonuçlanmıştır. Blok I uyduları, genellikle mevcut spesifikasyonlardan farklı olarak 63° eğimle yerine 55° eğimle döşenmiştir. Bu uydular, kontrol istasyonları tarafından çalıştırılan hidrazin iticileriyle manevra yapabilmektedirler.

İlk GPS uydusu, 22 Şubat 1978'de fırlatılarak Navstar 1 olarak bilinmektedir. Navstar 2'nin PRN 7 olarak bilinmesi gibi bu uydunun da PRN 4 olarak bilinmesi talihsiz bir komplikasyondur. Her bir GPS uydusunun bir dizi tanımlayıcısı bulunmaktadır, ancak en önemlisi PRN numarasıdır. Blok I uyduları, son yörüngede 845 kg ağırlığındaydı ve üç adet şarj edilebilir nikel-kadmiyum pil ile güçlendirilmiştir. Bu deneysel uydular, sonraki nesillerde yapılacak iyileştirmeler için yol göstermiştir. Örneğin, her uyduda bulunan rubidyum ve sezyum osilatörlerden oluşan yedek sistemler, saatlerin en hassas bileşenler olmadığını kanıtlamıştır. Ancak uyduların kendileri, sadece 3.5 günlük bağımsız çalışma için yeterli bilgiyi depolayabilmektedir ve kontrol bölümünden yapılan yüklemeler güvenli değildir. Navstar 7 hariç, 11 uydunun tamamı yörüngeye başarıyla oturtulmuştur. Tasarım ömrü 4.5 yıl olarak belirlenen Blok I uydularının gerçek ortalama ömürleri ise 8.76 yıl olmuştur. Bugün, çalışır durumda olan herhangi bir Blok I uydusu bulunmamaktadır.

2.3.2 Block II Uyduları

Şekil 2.6 Block II Uydusu 1989 – 1990 [2]

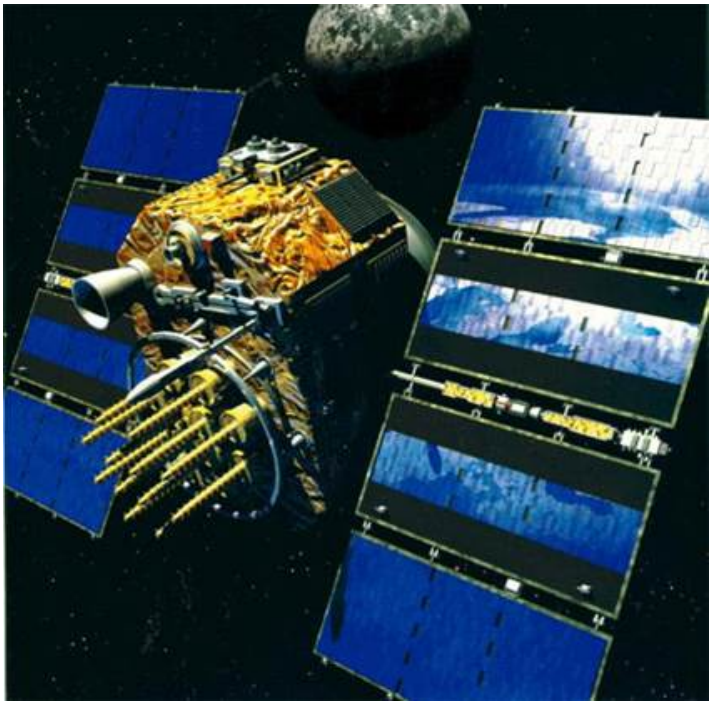
Block I'e göre bazı iyileştirmeler:

- 14 gün kontrol segmenti olmadan çalışma
- 7.3 yıl tasarım ömrü

Yeni nesil GPS uyduları, Blok II uyduları olarak bilinmektedir. İlk Blok II uydusu, ilk GPS uydusunun fırlatılmasından neredeyse 14 yıl sonra, 14 Şubat 1989'da Cape Canaveral'dan ayrılmıştır. Blok II uyduları, Blok I uydularına göre yaklaşık iki kat daha ağırdır ve ortalama görev süresi 6 yıl olan 7.5 yıllık bir tasarım ömrüne sahiptir. Bu uydular, kontrol segmentinden bir yükleme olmadan 14 güne kadar çalışabiliyor ve yüklemeleri şifrelenmiştir. Ayrıca, uyduların kendileri radyasyona karşı güçlendirilmiştir ve sinyalleri seçici kullanılabilirliğe tabidirler. Blok II uyduları, Rockwell International tarafından inşa edilmiştir ve 1989 ile 1990 yılları arasında 9 uydunun fırlatılmasını içermiştir. Ancak,

günümüzde hiçbir Blok II uydusu takımyıldızda yer almamaktadır ve sonuncusu 2007 yılında hizmet dışı bırakılmıştır.

2.3.3 Block IIA Uyduları



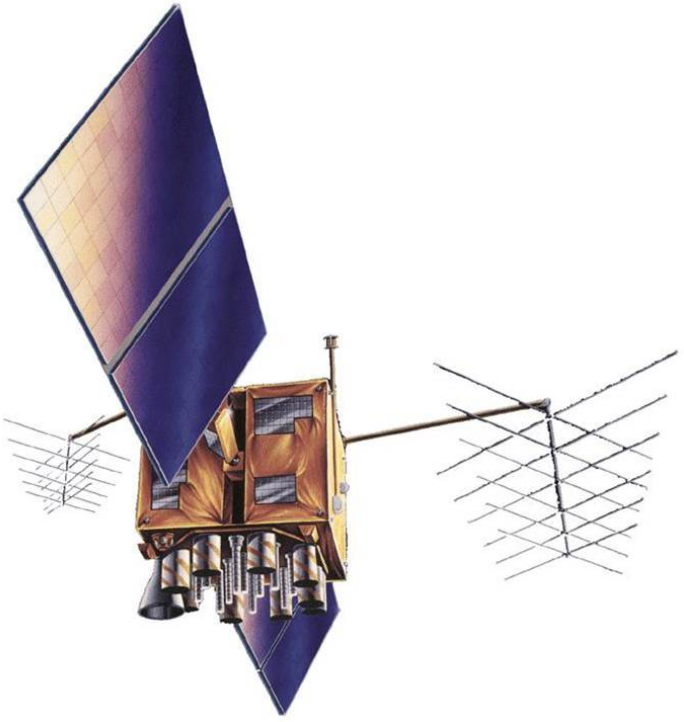
Şekil 2.7 Block IIA Uydusu 1990 – 1997 [2]

Block II'e göre bazı iyileştirmeler:

- bozulma olmadan 6 ay kontrol segmentsiz çalışma
- Radyasyon ile sertleştirilme

Blok IIA uydularının fırlatılmasına 1990 yılında başlanmıştır. Bu süre zarfında, 1990 ile 1997 yılları arasında, çeşitli seyrüsefer iyileştirmelerine sahip toplam 19 Blok IIA uydusu fırlatılmıştır. Blok IIA uyduları, Blok II uydularından daha fazla navigasyon mesajı depolayabilir ve bu nedenle 6 ay boyunca Kontrol Segmenti ile temas kurmadan çalışabilir. Ancak, bu durumda, yayın efemerisleri ve saat düzeltmeleri bozulabilir. Ne yazık ki, Blok IIA uydularının hiçbiri günümüzde takımyıldızda aktif olarak görev almamaktadır.

2.3.4 Block IIR Uyduları



Şekil 2.8 Block IIR Uydusu 1997-2004 [2]

Block IIA'e göre bazı iyileştirmeler:

- Uydular arası çapraz bağlantı aralığı (AutoNav)
- 3 rubidyum frekans standartları
- Tehlike Uyarı Uydu Sistemi (Distress Alerting Satellite System, DASS) kavram kanıtı

Bir sonraki Blok olan Blok IIR uydularının Ocak 1997'deki ilk fırlatılışı başarısız olmuştur, ancak Temmuz 1997'deki bir sonraki fırlatma başarılı olmuştur. Üçüncü nesil GPS uyduları Blok IIR uyduları olarak bilinmektedir ve "R" harfi, bu bloğun iyileştirilmiş sürümü olduğunu belirtir. Blok IIR uyduları, uydular arası bağlantı (AutoNav olarak adlandırılır) kullanmaları nedeniyle gelişmiş otonom navigasyon yeteneğine

sahiptir. Bu özellik, uçuş sırasında kendi düzeltmelerini yapmak için gemide yeniden programlanabilir işlemcilerin kullanılmasını içerir. Günümüzde, takımyıldızda Blok IIR uyduları bulunmaktadır.

2.3.5 Block IIR-M Uyduları

Şekil 2.9 Block IIR-M Uydusu 2005-2009 [2]

Block IIR'e göre bazı iyileştirmeler:

- 2. Sivil Sinyal L2 (L2C)
- L1/L2 üzerinde M-Kodu
- L5 Demo
- Anti-Jam Esnek Güç

Eylül 2005'te, Blok IIR-M olarak adlandırılan bir sonraki geliştirilmiş bloğun ilki fırlatılmıştır. Bu uydular, fırlatılmadan önce modifiye edilmiş olan Blok IIR uydularının bir versiyonudur. Yapılan değişikliklerle bu uydular, iki yeni kod yayınlama yeteneği kazanmıştır: yeni bir askeri kod olan M kodu, yeni bir sivil kod olan L2C kodu ve yeni bir taşıyıcı olan L5 kodu. Günümüzde, takımyıldızda Blok IIR-M uyduları bulunmaktadır.

2.3.6 Block IIF Uyduları

Şekil 2.10 Block IIF Uydusu 2010-2016 [2]

Block IIR-M'e göre bazı iyileştirmeler:

- 3. Sivil Sinyal L5
- 12 yıllık tasarım ömrü
- Geliştirilmiş rubidyum frekans standartları
- Doğrudan yörüngeye yerleştirme
- Operasyonel Tehlike Uyarı Uydu Sistemi (DASS) tekrarlayıcıları

Blok IIF uyduları L2C sinyali ve üçüncü sivil taşıyıcı, iyonosfer modellemesi için GPS'te önemli bir rol oynamaktadır çünkü iyonosfer etkilerini daha doğru bir şekilde hesaplamamıza

yardımcı olmaktadır. İki taşıyıcı ile bu modelleme başarılı bir şekilde gerçekleştirilebilir, ancak üçüncü taşıyıcının eklenmesi bu modellemeyi daha da iyileştirecektir.

Blok IIF uydu grubunun ilki 2010 yılının Mayıs ayında yörüngeye ulaşmıştır. GPS uydu takımyıldızında sürekli ve istikrarlı bir gelişme gözlenmiştir. İlk Blok IIF uydusu 2010 yazında fırlatılmış olup, tasarım ömürleri 12 ila 15 yıldır. Blok IIF uyduları, daha hızlı işlemcilere ve daha fazla belleğe sahiptir. Ayrıca, daha önce bahsedilen tüm sinyalleri, L5 taşıyıcısı da dahil olmak üzere, yayınlarlar. Bu sinyaller, Blok IIR-M'de gösterilmiş ve tüm Blok IIF uydularından kullanılabilir. Blok IIF uyduları, yaşlandıkça Blok IIA uydularının yerini almıştır. Yerleşik navigasyon veri birimleri (Navigation Data Units ,NDU), geliştirilmiş yayın efemerisi ve saat düzeltmeleri ile yeni navigasyon mesajlarının oluşturulmasını destekler. Blok IIR uyduları gibi, Blok IIF uyduları da yörüngede yeniden programlanabilmektedir.

2.3.7 Block III Uyduları

Şekil 2.11 Block III Uydusu 2018-? [2]

Block IIF'e göre bazı iyileştirmeler:

- Artırılmış Dünya kapsama gücü
- 15 yıl tasarım ömrü
- 4. Sivil Sinyal (L1C)
- Yerleşik LRA
- Daha verimli güncellemeler için 2 ila 4 çapraz bağlantı anteni
- Spot ışın

Blok III uyduları, hizmet dışı bırakılan eski uyduların yerini almaktadır. Şu anda yörüngede IIIA uyduları bulunmaktadır. Bu blok üç kademeli olarak konuşlandırılacaktır. Bunlardan ilki IIIA olarak bilinmektedir. Düşmanların karıştırmasına (jamming) karşı dayanıklı olacaktır. Sonraki iki artış IIIB ve Blok IIIC'dir. IIIB uyduları tarafından yayınlanan sinyaller için daha yüksek güç planlanmaktadır. IIIB ve IIIC uyduları ayrıca Tehlike Uyarı Uydu Sistemi (Distress Alerting Satellite System, DASS) tekrarlayıcıları taşıyacaktır. Tüm GPS takımyıldızında DASS tekrarlayıcıları bulunduğunda, uydu destekli arama ve kurtarma için küresel kapsama alanı olacak ve en az dört DASS donanımlı uydu Dünya'nın herhangi bir yerinden her zaman görülebilecektir. Bu sistem uluslararası Cospas-Sarsat uydu destekli arama ve kurtarma (search and rescue, SAR) sistemini geliştirecek ve benzer şekilde planlanan Rus (SAR/GLONASS) ve Avrupa (SAR/Galileo) sistemleriyle birlikte çalışabilir olacaktır.

Blok III uyduları, uydular arası menzil ve aktarımı desteklemek için çapraz bağlantı yeteneğine; telemetri, izleme ve kontrol (telemetry, tracking and control, TT&C) yeteneğine sahip olacaktır. Blok IIIB uyduları, iki ila dört yönlü çapraz bağlantı antenine sahip olacaktır. Bu, her uydunun güncellenmek için bir yer anteninin menzilinde olmasını gerektirmek yerine tek bir yer istasyonundan güncellenebilecekleri anlamına gelmektedir. Bu ve yüksek hızlı yükleme ve indirme antenleri, yükleme sıklığının her 12 saatte bir yerine her 15 dakikada bire çıkarılmasına yardımcı olabilir. Her bir Blok III uydusu üç adet geliştirilmiş rubidyum frekans standardına (saat) sahip olacak ve yeni bir saat, yani hidrojen maseri için

dördüncü bir yuva mevcut olacaktır. Tüm Blok III uydularının yerleşik Lazer Retroreflektör Dizilerine (Laser Retroreflector Arrays, LRA) (diğer adıyla retro-reflektörler) sahip olacağı 2010 yılında belirlenmiştir. Bu faydalı yük ile elde edilebilecek uydu lazer takibi, saat hatası ile efemeris hatasını ayırt etmenin mümkün olacağı verileri sağlayacaktır Benzer LRA'lar Rus (GLONASS) ve Avrupa (Galileo) sistemleri için de planlanmıştır.

Bu uydular için L1 taşıyıcısı üzerinde L1C olarak bilinen yeni bir sivil sinyalin yayınlanmasını içeren bir plan vardır. Bu sinyal, Galileo'nun Açık Hizmet Sinyali ve Japonya'nın Quazi-Zenith Uydu Sistemi (QZSS) ile birlikte çalışabilirliği en üst düzeye çıkarmak için uluslararası işbirliği ile tasarlanmıştır. Daha önceki bloklarda mevcut olan M kodu, L5, P kodu ve C/A kodu gibi kodlar Blok III uydularından artan güçle yayınlanacaktır.

M kodunun yayını ilginç bir şekilde değişecektir. Tıpkı Blok IIR-M uydularında olduğu gibi tüm dünyayı kapsayacak şekilde geniş bir açıyla yayılmaya devam edecek, ancak Blok IIIC M kodu ayrıca yönlü bir spot ışın üretmek için oldukça büyük bir konuşlandırılabilir yüksek kazançlı antene sahip olacaktır. Spot ışın, geniş açılı M-kod yayınına (-158 dBW) kıyasla yaklaşık 100 kat daha fazla güce (-138 dBW) sahip olacaktır. Birkaç yüz kilometre çapındaki bir bölgeye yönelik anti-parazit (anti-jam, AJ) yeteneğine sahip olacaktır. İki antene sahip olmanın bir yan etkisi de GPS uydusunun spot ışınının içinde kalanlara aynı pozisyonu işgal eden iki GPS uydusu gibi görünmesidir.[2]

Tablo 2.2 Uyduların Özeti

Blok	**Fırlatılma**	**Uydu durumu**				**Yörüng. ve işler**
		Başarılı	**Başarısız**	**Yapım**	**Tasarı**	
I	1978-1985	10	1	0	0	0
II	1989-1990	9	0	0	0	0
IIA	1990-1997	19	0	0	0	9
IIR	1997-2004	12	1	0	0	12
IIR-M	2005-2009	8	0	0	0	7
IIF	2010 sonrası	3	0	10	0	3
IIIA	2014 sonrası	0	0	0	12	0
IIIB	-	0	0	0	8	0
IIIC	-	0	0	0	16	0
Toplam		61	2	10	36	31

2.3.8 GPS Modernizasyonu Özeti

- 1972'de, ABD Hava Kuvvetleri Holloman Hv. K. Üssü'nde GPS alıcılarının prototipleri için uçuş testleri yapılmıştır.
- 1978'de, ilk Blok-I GPS uydusu fırlatılmıştır.
- 1983'te, Kore Hava Yolları'nın Sovyet hava sahasına sapması sonucu KAL 007 uçağı düşürülmüş ve GPS'in sivil kullanıma açılması hızlandırılmıştır.
- 1985'te, deneysel Blok-I uyduları fırlatılmıştır.
- 1989'da, ilk çağdaş Blok-II uydusu fırlatılmıştır.
- 1990-1991 Körfez Savaşı, GPS teknolojilerinin aktif olarak kullanıldığı ilk büyük çatışma olmuştur.
- 1992'de, GPS sisteminin yönetimi 2. Uzay Kanatları'na devredilmiştir.
- 1993'te, GPS'nin tam operasyonel yeteneği elde edilmiştir.
- 1995'te, GPS'in tam operasyonel kabiliyeti ilan edilmiştir.
- 1996'da, GPS'in çift kullanımlı sistem olarak ilan edilmesi ve bir GPS yürütme kurulu oluşturulması gerçekleşmiştir.
- 1998'de, Al Gore'un GPS'i geliştirmek için açıkladığı plânlar duyurulmuştur.
- 2000'de, "Seçici Kullanılabilirlik" durumunun sona erdirilmiştir.
- 2004'te, ABD'nin Galileo sistemi ile işbirliği anlaşması yapılmıştır.
- 2004'te, Uzay-Tabanlı konumlama ve Zamanlama için Ulusal Yürütme Komitesi'nin oluşturulması gerçekleşmiştir.
- 2005'te, ilk çağdaş GPS uydusu fırlatılmış ve L2C sinyali yayını başlamıştır.

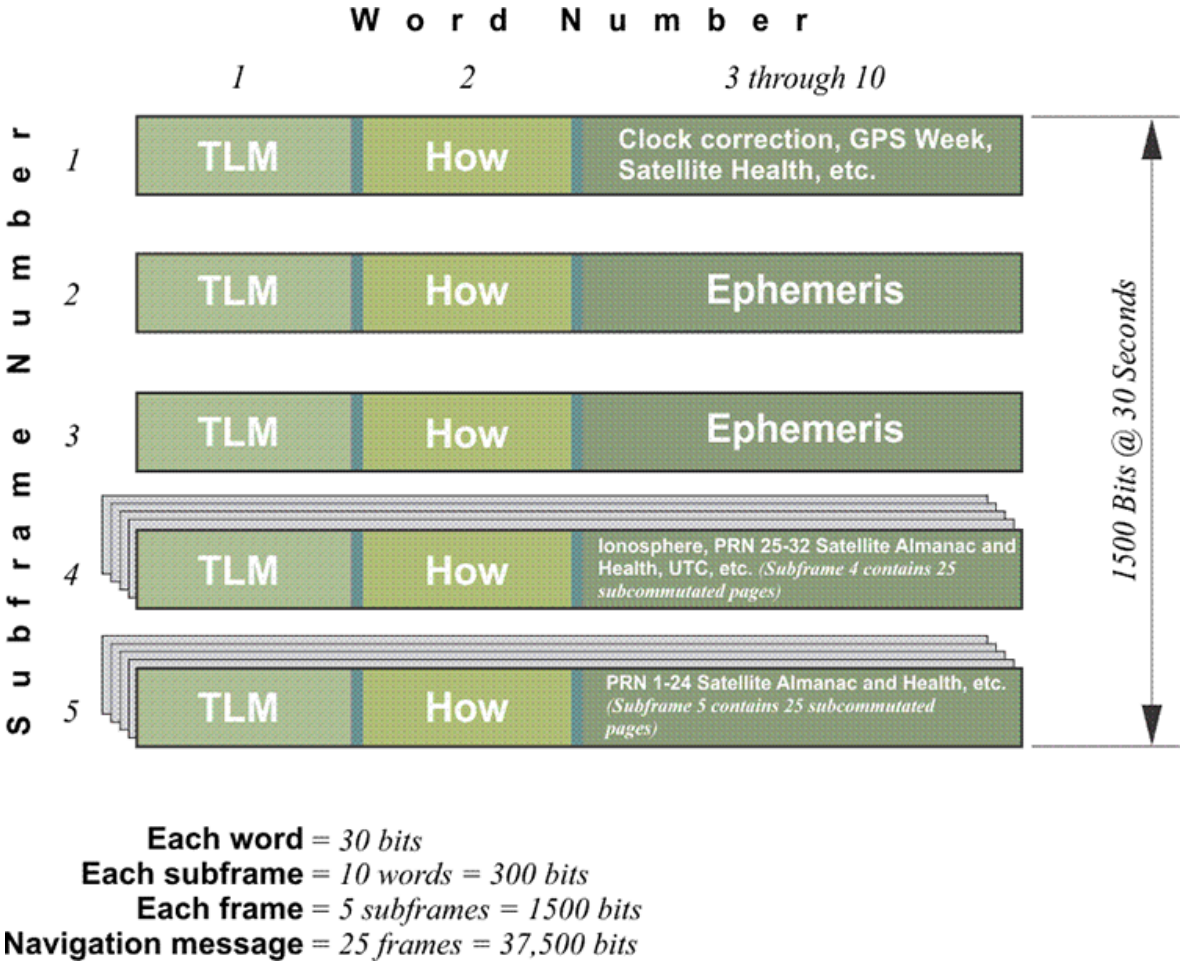
- 2007'de, ana bilgisayar tabanlı Yer Segmenti Kontrol Sistemi'nin (mainframe-based Ground Segment Control System) evriminin planlaması yapılmıştır.
- 2009'da, bazı GPS uydularının başarısızlık riskine dair Sayıştay raporu yayımlanmıştır.
- 2009'da, Hava Kuvvetleri Uzay Komutanlığı'nın GPS yetersizliği hakkındaki açıklamaları yapılmıştır.
- 2010'da, GPS Yeni Nesil Operasyonel Kontrol Sistemi'nin (OCX) geliştirilmesi için sözleşme imzalanmıştır.

2.4 Küresel Konumlandırma Sinyallerinin İçeriği

GPS'in temel amacına yönelik olarak uydu ve alıcı arasındaki iletişim NAV mesajıdır. NAV mesajı GPS mesajı olarak da bilinir. Alıcıların konumlarını belirlemek için ihtiyaç duydukları bazı bilgileri içerir. Bugün, GPS uyduları tarafından yayınlanan birkaç NAV mesajı vardır ancak eski navigasyon (NAV) mesajı GPS'in dayandığı temel dayanaklardan biri olmaya devam etmektedir. NAV kodu hem L1 hem de L2 GPS taşıyıcılarında 50 Hz gibi düşük bir frekansta yayınlanır. Efemeris adı verilen GPS uydularının konumu hakkında bilgi ve hem zaman dönüşümlerinde hem de saat düzeltmeleri adı verilen ofsetlerde kullanılan verileri taşır. Hem GPS uydularının hem de alıcılarının üzerinde saat bulunur. Ayrıca yörüngedeki uyduların sağlık durumunu ve iyonosfer hakkındaki bilgileri de iletir. İyonosfer, troposfer ile birlikte, GPS sinyallerinin kullanıcıya ulaşması için içinden geçmesi gereken bir atmosfer tabakasıdır. Bir GPS alıcısına, takımyıldızdaki tüm uyduların koordinatlarını yaklaşık birkaç kilometre doğrulukla hesaplamak için yeterli küçük efemeris bilgi parçacıkları sağlayan almanak adı verilen verileri içerir. Navigasyon kodu ya da mesajı, GPS alıcılarına bilmeleri gereken en önemli şeylerden bazılarını bildiren bir araçtır.

Navigasyon mesajının tamamı, Ana Çerçeve, Şekil 2.12'de görüldüğü gibi 25 çerçeve (frame) içerir. Her çerçeve 1500 bit uzunluğundadır ve beş alt çerçeveye bölünmüştür. Her alt çerçeve 10 kelime (word) içerir ve her kelime 30 bitten oluşur. Bu nedenle, Navigasyon

mesajının tamamı 37.500 bit içerir ve saniyede 50 bitlik bir hızda, tamamen soğuk bir başlangıçta yayınlanması ve alınması 12.5 dakika sürer. Başka bir deyişle, her şeyi almak anlık değildir. Alıcının Navigasyon Mesajını güncellemesi biraz zaman alır.



Şekil 2.12 Navigasyon (NAV) Mesajı [2]

Eski Navigasyon Mesajı, beş alt çerçevede organize edilmiştir. İlk çerçeve TLM (Telemetry) olarak adlandırılmıştır, bu çerçeve genellikle uydu hakkında telemetri verilerini içerir. HOW (Handover Word) adı verilen ikinci çerçeve, devir (handover) bilgilerini taşır. Şekil 2.12'de sağ tarafta, birinci alt çerçevede saat düzeltmesi, GPS uydu sağlığı ve benzeri bilgiler bulunmaktadır. İkinci ve üçüncü çerçeveler genellikle efemeris verilerini içerir. Dördüncü ve beşinci çerçeveler, iyonosfer ve PRN uydu numaraları ve almanak verileri ile ilgilidir. Dördüncü çerçevedeki 25'ten 32'ye kadar olan PRN numaraları, 25 numaradan 32 numaraya kadar olan uydu almanaklarının burada bulunacağını gösterir. Beşinci çerçevedeki 1'den 24'e

kadar olan PRN'ler ise bu uyduların almanaklarını, yani efemeritlerinin bir kısmını içerir. Bu düzenleme, Navigasyon Mesajının temel bileşenlerini organize etmek ve kullanıcıya gerekli olan bilgileri iletmek için tasarlanmıştır.

Bu mesajın temel amacı, uydunun alıcıya önemli bilgileri iletmek için esas bir araç olmasıdır. Alıcı, uydudan gelen sinyali aldıktan sonra, NAV mesajı vasıtasıyla uydunun bulunduğu konumu öğrenir. Efemeris, uydunun koordinat sistemini tanımlar ve alıcıya uydunun belirli bir zamandaki konumunu bildirir. Saat düzeltmesi, uydunun alıcıya uydu üzerindeki saati belirtme yöntemlerinden biridir. İyonosfer bilgisi, alıcının belirli bir uydudan aldığı sinyalin atmosferdeki etkilerini hesaplamasına yardımcı olur. Bu bilgi, sinyalin atmosferdeki yolculuğu sırasında meydana gelen zaman gecikmelerini düzeltmek için kullanılır. Bu temel unsurlar, GPS alıcısının uydu sinyallerini alırken ve doğru konum bilgisini türetirken kritik bilgileri sağlar.

NAV mesajında yer alan bilgilerin bazı yönlerinin doğruluğu zamanla bozulur. Bir GPS alıcısının üç boyutlu konumundaki değişim oranına çevrildiğinde, dakikada yaklaşık 4 cm'dir. Bu nedenle, mesajın çok eskimesini önleyecek mekanizmalar mevcuttur. Örneğin, her iki saatte bir, efemeris ve saatin parametreleri olan 1, 2 ve 3. alt çerçevelerdeki veriler güncellenir. Alt çerçeve 4 ve 5'teki veriler, yani almanaklar her altı günde bir yenilenir. Bu güncellemeler, izleme ve hesaplama muadilleriyle birlikte Kontrol Segmenti olarak bilinen, dünyanın dört bir yanındaki hükümet yükleme tesisleri tarafından sağlanır. Kontrol Segmentinden her bir uyduya gönderilen bilgi, uydular arasında yol alır ve NAV mesajında kullanıcılara geri döner.

NAV mesajı, özellikle 1. ve 4. alt çerçevelerde, GPS Zamanı ile Eşgüdümlü Evrensel Zaman (Coordinated Universal Time, UTC) arasında senkronizasyon için çok önemli olan zamana duyarlı bilgiler içerir. GPS Saati GPS sistemi için standart olarak hizmet verirken, UTC küresel olarak tanınmaktadır. Neredeyse aynı oranlara sahip olmalarına rağmen, dünyanın dönüşüne uyması için UTC'ye periyodik olarak eklenen artık saniyeler nedeniyle farklılıklar mevcuttur. Ancak, GPS Saati 6 Ocak 1980'den itibaren artık saniye olmaksızın sürekliliğini korur. NAV mesajının 4. Alt Çerçevesi bu ilişkiyi tanımlar ve gelecekteki artık saniyeleri

tahmin eder. Ayrıca, alıcı ve uydu arasındaki saat senkronizasyonuna yardımcı olur, bu da doğru zaman tutma için çok önemlidir. Kontrol Segmenti, uydu saatinin kaymasını önlemek için saat düzeltmelerini yöneterek GPS Saati ile bir milisaniye eşiği içinde hizalanmayı sağlar ve böylece uydu ömrünü uzatır. Bu mekanizma alıcılara zaman standartlarını etkin bir şekilde korumak için gerekli araçları sağlar.

NAV Mesajının 2. ve 3. alt çerçeveleri, zaman içinde Dünya'ya göre uydu konumlarını detaylandıran zamana duyarlı efemeris verileri sağlar. Doğru konumlandırma için çok önemli olan bu bilgiler, alıcıların WGS84 sisteminde uydu koordinatlarını hesaplamasına olanak tanıyan yarı büyük eksen ve eksantriklik gibi yörünge unsurlarını içerir. Keplerian görünmesine rağmen, uydu yörüngeleri yerçekimi kuvvetleri nedeniyle sapma gösterir ve doğruluk için periyodik güncellemeler gerektirir. Bu alt çerçevelerdeki Veri Efemeris Yayını (Issue of Data Ephemeris, IODE) bir zaman damgası görevi görerek alıcıların uydu kontrol noktalarından kesin mesafeler türetmesine yardımcı olur.

NAV Mesajının 4. Alt Çerçevesi atmosferik düzeltmeyi ele alır ve iyonosferin neden olduğu sinyal gecikmelerini azaltmak için gerekli verileri sağlar.

NAV Mesajının 4. ve 5. alt çerçeveleri GPS uydularının yerini belirlemek için çok önemli olan almanak verilerini içerir. 4. alt çerçeve 25-32 PRN numaralarını, 5. alt çerçeve ise 1-24 PRN numaralarını kapsar. Kontrol Bölümü bu bilgileri düzenli olarak günceller ve alıcıların görünür uyduları hızlı bir şekilde tanımlamasına yardımcı olur. Almanak verileri, efemeritlerden daha az ayrıntılı olsa da, alıcı başlatma sırasında uydu listeleri oluşturmak için yeterli kaba yörünge parametreleri sağlar. Sıcak başlatma, daha hızlı uydu alımı için artık almanak ve konum verilerini kullanırken, soğuk başlatma ön bilgi olmadan uyduları aramayı içerir. İlk düzeltmeye kadar geçen süre(Time to first fix, TTFF) değişir: soğuk başlatmalar için en uzun, sıcak başlatmalar için en kısa ve sıcak başlatmalar için en hızlı süre.

Alt Çerçeve 1, kullanımdan önce uydunun çalışabilirliğini değerlendirmek için çok önemli olan uydu sağlık bilgilerini içerir. Kontrol Segmenti tarafından periyodik olarak güncellenen bu veriler, alıcıları herhangi bir arıza veya yaklaşan bakım faaliyetleri hakkında bilgilendirerek güvenilir konumlandırma sağlar.

Bu beş alt çerçevenin her biri aynı iki kelimeyle başlar: telemetri kelimesi (TLM) ve devir kelimesi (HOW). NAV mesajındaki neredeyse diğer her şeyin aksine, bu iki kelime uydunun kendisi tarafından üretilir. GPS zamanı her Pazar gece yarısı (saat 0:00) yeniden başlar. Bu veriler, GPS zamanının bir önceki Pazar günü saat 0:00'da yeniden başlatılmasından bu yana geçen süreyi içerir.

TLM her alt çerçevedeki ilk kelimedir. Devam etmekte olan Kontrol Segmentinden yükleme durumunu gösterir ve efemeris verilerinin yaşı hakkında bilgi içerir. Ayrıca 10001011 adresinde sabit ve değişmeyen 8 bitlik bir önsöze sahiptir ve bir dize alıcının her alt çerçevenin başlangıcını güvenilir bir şekilde bulmasına yardımcı olur.

HOW alıcıya diğer şeylerin yanı sıra GPS haftasının zamanı (time of week, TOW) ve alt çerçevenin numarası hakkında bilgi sağlar. Örneğin, HOW'un Z sayısı (dahili olarak türetilmiş 1,5 saniyelik bir epok) alıcıya uydunun konumlandırma kodlarının üretiminde tam olarak nerede durduğunu söyler.

Telemetri (TLM) kelimesi, kontrol segmentinin yüklenme durumunu, işlemde olup olmadığını gösterir. Bu, alıcınızın bunu bilmesini sağlar. Ayrıca, veri dizisindeki her kelimenin başlangıcını bilmenizi sağlar. HOW kelimesi birkaç yönden yararlıdır, ancak muhtemelen en önemlisi alıcınıza uydunun kod yayınında nerede olduğunu söylemektir.

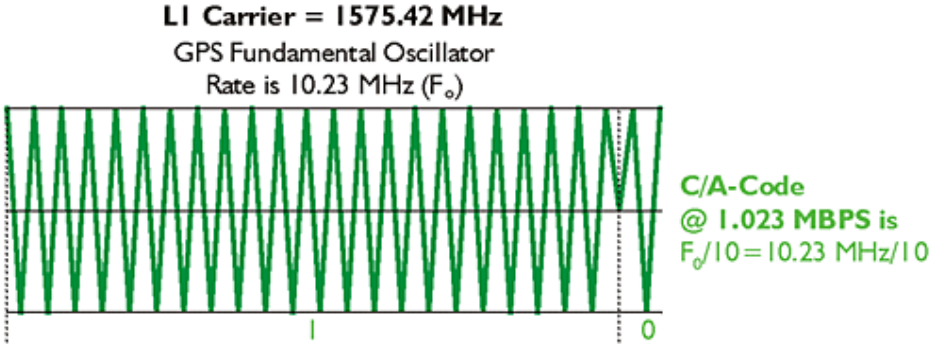
2.5 Küresel Konumlandırma Sistemi Sinyal Haberleşmesi

Orijinal GPS tasarımı iki menzil kodu (ranging code) içerir: halka açık olan Kaba/Algılama kodu (Coarse/Acquisition, C/A) ve genellikle askeri uygulamalar için ayrılmış olan Hassas kod (Precision Code , P-Code).

2.5.1 C/A Kodu

C/A kodu, saniyede 1,023 megabit (Mbit/s) hızla iletildiğinde her milisaniyede bir tekrar eden 1.023 bit uzunluğunda bir sözde rasgele koddur. Bu diziler yalnızca tam olarak

hizalandıklarında eşleşir veya güçlü bir şekilde korelasyon gösterir. Her uydu, başka bir uydunun PRN koduyla iyi bir korelasyon göstermeyen benzersiz bir PRN kodu iletir. Başka bir deyişle, PRN kodları birbirlerine oldukça ortogonaldir. Bu, alıcının aynı frekanstaki birden fazla uyduyu tanımasını sağlayan bir Kod Bölmeli Çoklu Erişim (CDMA) biçimidir.



Şekil 2.13 C/A Kodu [2]

2.5.2 P Kodu

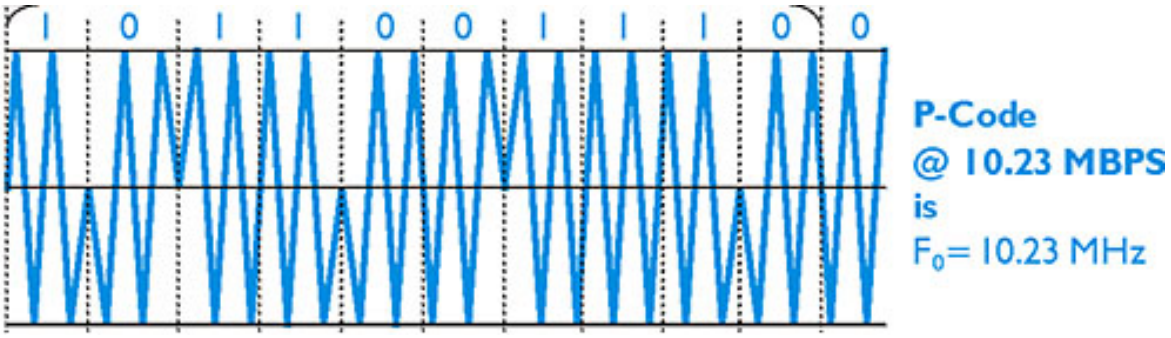
P-kodu da bir PRN'dir, ancak her uydunun P-kodu PRN kodu 6,1871 × 10^{12} bit uzunluğundadır (6.187.100.000.000 bit) ve haftada yalnızca bir kez tekrarlanır (10,23 Mbit/s hızında iletilir). P-kodunun aşırı uzunluğu korelasyon kazancını artırır ve Güneş Sistemi içindeki herhangi bir menzil belirsizliğini ortadan kaldırır. Ancak kod o kadar uzun ve karmaşıktır ki bir alıcının tek başına bu sinyali doğrudan alıp senkronize edemeyeceği düşünülmüştür. Alıcının önce nispeten basit C/A koduna kilitlenmesi ve ardından mevcut zamanı ve yaklaşık konumu elde ettikten sonra P kodu ile senkronize olması bekleniyordu.

C/A PRN'leri her uydu için benzersizken, P-kodu PRN'si aslında yaklaşık 2,35 × 10^{14} bit uzunluğunda (235.000.000.000.000 bit) bir ana P-kodunun küçük bir bölümüdür ve her uydu ana kodun kendisine tahsis edilen bölümünü tekrar tekrar iletir.

Yetkisiz kullanıcıların aldatma (spoofing) adı verilen bir işlemle askeri sinyali kullanmasını ya da potansiyel olarak müdahale etmesini önlemek için P-kodunun şifrelenmesine karar verildi. Bu amaçla P-kodu özel bir şifreleme dizisi olan W-kodu ile modüle edilerek Y-kodu

oluşturuldu. Y kodu, sahteciliğe karşı koruma modülünün ”açık” duruma getirilmesinden bu yana uyduların ilettiği koddur. Şifrelenmiş sinyal P(Y)-kodu olarak adlandırılır.

W-kodunun ayrıntıları gizli tutulmaktadır, ancak P-koduna yaklaşık 500 kHz'de uygulandığı bilinmektedir, bu da P-kodunun kendisinden yaklaşık 20 kat daha yavaş bir orandır. Bu durum şirketlerin W-kodunun kendisi hakkında bilgi sahibi olmadan P(Y) sinyalini izlemek için yarı-kodsuz yaklaşımlar geliştirmelerine olanak sağlamıştır.



Şekil 2.14 P Kodu [2]

2.5.3 Frekans Bilgisi

Menzil kodlarının ve navigasyon mesajının uydudan alıcıya ulaşabilmesi için bir taşıyıcı frekans üzerinde modüle edilmeleri gerekir. Orijinal GPS tasarımında iki frekans kullanılır; biri 1575,42 MHz'de (10,23 MHz × 154) L1 olarak adlandırılır; ve ikincisi 1227,60 MHz'de (10,23 MHz × 120) L2 olarak adlandırılır. 2009 da GPS IIF uydularının kullanılmasıyla birlikte gelen bir havacılık navigasyon bandı olan L5 frekansı ise 1176,45 MHz (10,23 MHz × 115) de yayın yapar.

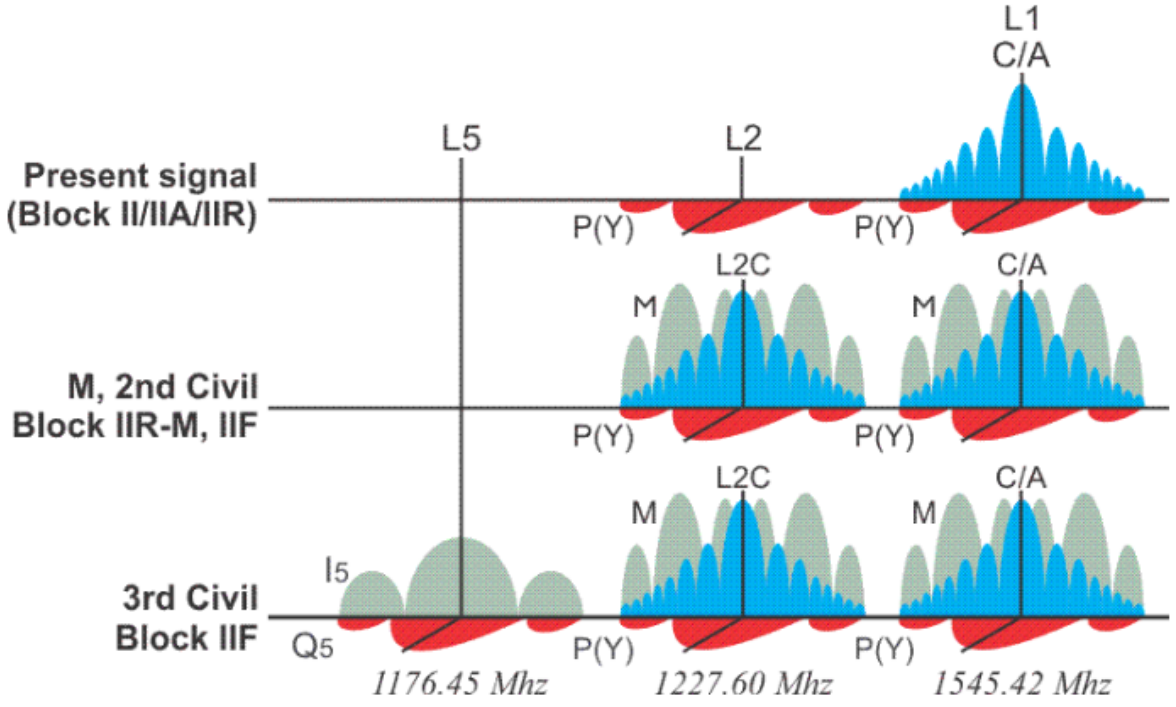
C/A kodu L1 frekansında Bi-Phase Shift Key (BPSK) modülasyon tekniği kullanılarak 1,023 MHz sinyal olarak iletilir. P(Y)-kodu hem L1 hem de L2 frekanslarında aynı BPSK modülasyonu kullanılarak 10,23 MHz sinyal olarak iletilir, ancak P(Y)-kodu taşıyıcısı C/A taşıyıcısı ile kuadraturdadır; yani 90° faz dışıdır.

Artıklık ve karıştırmaya karşı artan direncin yanı sıra, bir uydudan iletilen iki frekansa sahip olmanın kritik bir yararı, doğrudan ölçme ve dolayısıyla o uydu için iyonosferik gecikme

hatasını ortadan kaldırma yeteneğidir. Böyle bir ölçüm olmadan, GPS alıcısı genel bir model kullanmalı ya da başka bir kaynaktan (Geniş Alan Artırma Sistemi veya EGNOS gibi) iyonosferik düzeltmeler almalıdır. Hem GPS uydularında hem de GPS alıcılarında kullanılan teknolojideki gelişmeler, iyonosferik gecikmeyi sinyalde kalan en büyük hata kaynağı haline getirmiştir. Bu ölçümü yapabilen bir alıcı önemli ölçüde daha doğru olabilir ve tipik olarak çift frekanslı alıcı olarak adlandırılır.

2.5.4 GPS Sinyal Özellikleri

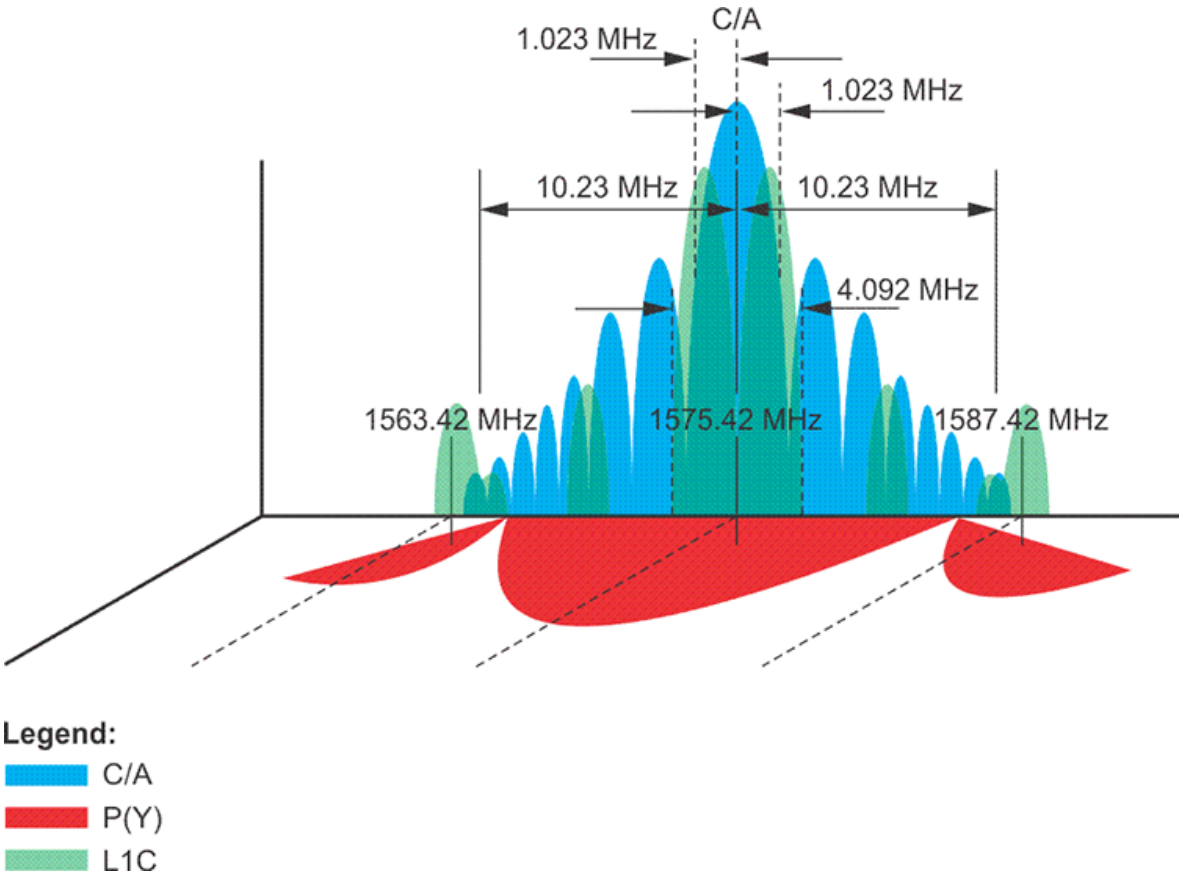
Sivil kullanım için tasarlanmış dört GPS sinyali özelliği vardır. Piyasaya çıkış tarihlerine göre bunlar şöyledir: L1 C/A , L2C , L5 ve L1C. L1 C/A aynı zamanda eski sinyal olarak da adlandırılır ve şu anda çalışır durumdaki tüm uydular tarafından yayınlanır. L2C, L5 ve L1C modernize edilmiş sinyallerdir ve yalnızca daha yeni uydular tarafından yayınlanmaktadır.



Şekil 2.15 GPS Sinyallerinin Uydulara Göre Değişimi [2]

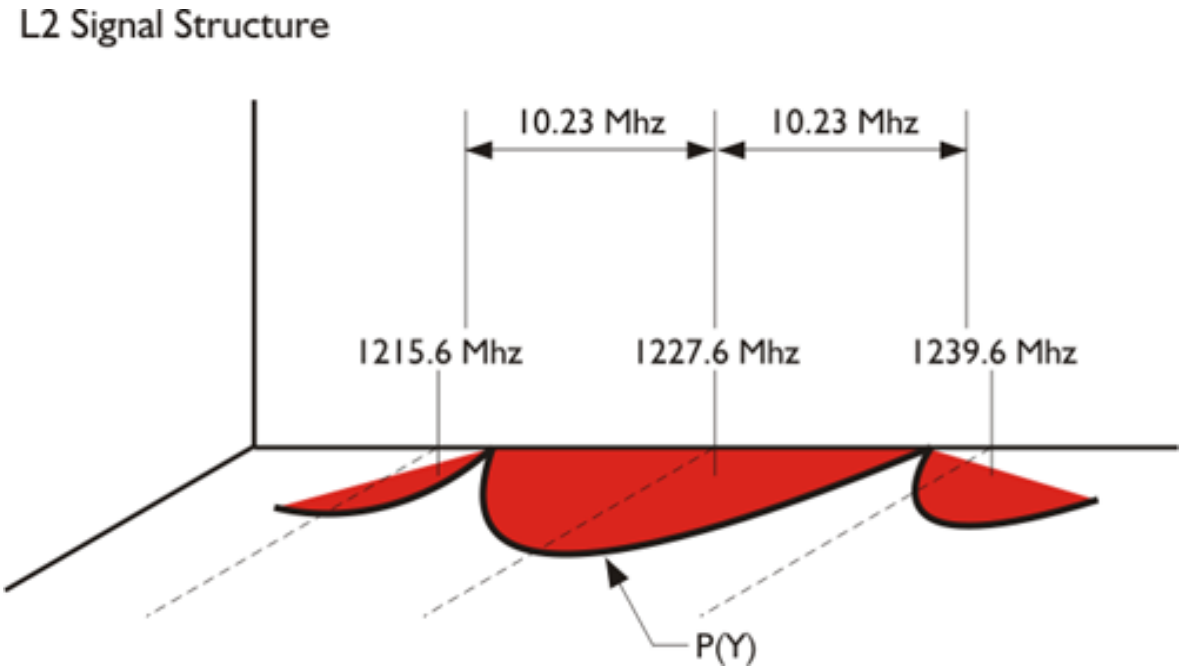
2.5.41. L1 C/A L1 C/A sinyali en eski GPS sinyalidir. İki bölümü vardır: Kaba/Algılama Kodu (C/A) ve Hassas Kod (P-kodu). P kodu askeri kullanım için ayrılmıştır, C/A ise

halka açıktır. L1 sinyali 1575,42 MHz frekansını kullanır. L1 en eski ve en yerleşik sinyal olduğundan, en ucuz GPS üniteleri bile bu sinyali alabilmektedir. Bununla birlikte, frekansı nispeten yavaş olduğu için engelleri aşmada çok etkili değildir.



Şekil 2.16 GPS L1 C/A Sinyalleri Spektrumu [2]

2.5.42. L2 L2 frekansı L1'den sonra uygulamaya konmuştur. L2, L1'den daha hızlı olan 1227,60 MHz frekansını kullanır. Bu, sinyalin bulut örtüsü, ağaçlar ve binalar gibi engellerden daha iyi geçmesini sağlar. Öncülü olan L1 frekans bandından farklı olarak L2 sistemi, öncelikle askeri uygulamalar için şifreli P(Y) kodunun kullanımını başlatmıştır. Bu şifreli kodu daha fazla güvenlik ve hassasiyet sunarak navigasyon, hedefleme ve zamanlama işlemlerinde askeri kullanıcılar için paha biçilmez hale getirmiştir. Ayrıca, L2 sistemi hem L1 hem de L2 sinyallerini alabilen çift frekanslı alıcıların geliştirilmesine olanak sağlayarak daha doğru konumlandırma ve iyonosferik bozulmalara karşı daha iyi direnç sağlamıştır.



Şekil 2.17 GPS L2 Sinyalleri Spekturumu [2]

2.5.43. L2C L2C ilk olarak Kaba Alım (C/A) sinyali için kullanılan L1 frekansından farklı bir frekansta iletilmek üzere geliştirilmiş, GPS içerisindeki bir sivil kullanım sinyalidir. Uydu üzerinde yeni bir donanım gerektirdiğinden, yalnızca Blok IIR-M olarak adlandırılan ve daha sonra tasarlanan uydular tarafından iletilir. L2C sinyalinin görevi seyrüsefer doğruluğunu arttırmak, kolay takip edilebilir bir sinyal sağlamak ve yerel parazit durumunda yedek sinyal olarak hareket etmektir.

C/A kodunun aksine, L2C menzil bilgisi sağlamak için iki farklı PRN kod dizisi içerir; Sivil Orta uzunlukta kod (CM olarak adlandırılır) ve Sivil Uzun uzunlukta kod (CL olarak adlandırılır). CM kodu 10.230 bit uzunluğundadır ve her 20 ms'de bir tekrarlanır. CL kodu 767.250 bit uzunluğundadır ve her 1.500 ms'de bir tekrarlanır. Her bir sinyal saniyede 511.500 bit (bit/s) olarak iletilir, ancak 1.023.000 bit/s'lik bir sinyal oluşturmak için birlikte çoğullanırlar.

CM CNAV Navigasyon Mesajı ile modüle edilir , CL ise herhangi bir modüle edilmiş veri içermez ve verisiz dizi olarak adlandırılır. Uzun, verisiz dizi L1 C/A kodundan yaklaşık 24 dB daha fazla korelasyon (250 kat daha güçlü) sağlar.

C/A sinyali ile karşılaştırıldığında, L2C 2,7 dB daha fazla veri kurtarma ve 0,7 dB daha fazla taşıyıcı izleme özelliğine sahiptir, ancak iletim gücü 2,3 dB daha zayıftır.

CNAV SEYRÜSEFER MESAJI

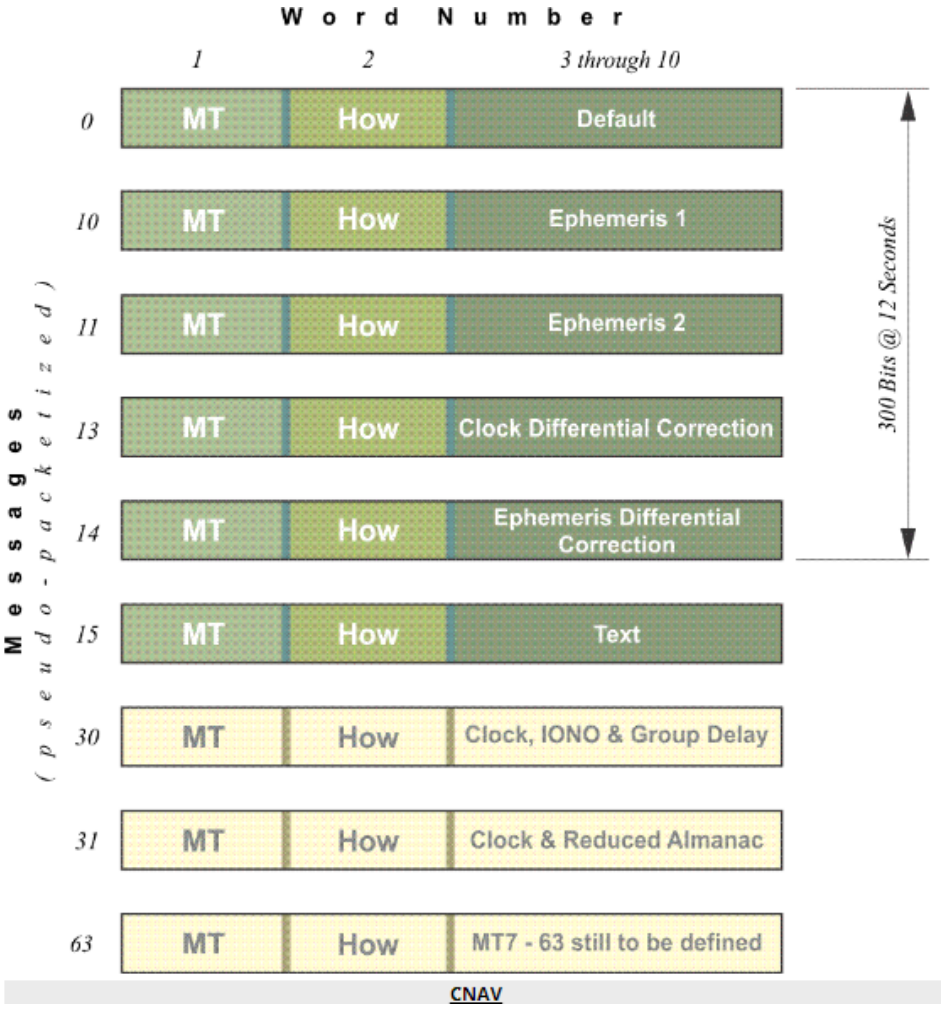
CNAV verileri orijinal NAV navigasyon mesajının yükseltilmiş bir versiyonudur. NAV verilerine göre daha yüksek hassasiyetli gösterim ve nominal olarak daha doğru veriler içerir. Aynı tür bilgiler (Zaman, Durum, Efemeris ve Almanak) hala yeni CNAV formatı kullanılarak iletilir, ancak bir çerçeve / alt çerçeve mimarisi kullanmak yerine, 12 saniyelik 300 bitlik mesaj paketlerinden oluşan yeni bir sözde paketleştirilmiş formata sahiptir.

CNAV'de her dört paketten ikisi efemeris verisidir ve her dört paketten en az biri saat verisi içerecektir, ancak tasarım çok çeşitli paketlerin iletilmesine izin vermektedir. 32 uyduluk bir takımyıldızı ve gönderilmesi gerekenlerin mevcut gereksinimleri ile bant genişliğinin %75'inden daha azı kullanılmaktadır. Ve mevcut paket türlerinin sadece küçük bir kısmı tanımlanmıştır. Bu da sistemin büyümesini ve gelişmeleri bünyesine katmasını sağlamaktadır.

Yeni CNAV mesajında birçok önemli değişiklik vardır:

- İleri Hata Düzeltme (FEC) 1/2 oranında bir konvolüsyon kodunda kullanılır, böylece navigasyon mesajı 25 bit/s iken, 50 bit/s'lik bir sinyal iletilir.
- GPS hafta numarası artık 13 bit ya da 8192 hafta olarak temsil ediliyor ve sadece 157.0 yılda bir tekrarlanıyor, yani bir sonraki sıfıra dönüş 2137 yılına kadar gerçekleşmeyecek. Bu, L1 NAV mesajının her 19,6 yılda bir sıfıra dönen 10 bitlik hafta numarası kullanımına kıyasla daha uzundur.
- GPS-GNSS zaman ofsetini içeren bir paket vardır. Bu, her ikisi de desteklenen Galileo ve GLONASS gibi diğer küresel zaman aktarım sistemleriyle birlikte çalışabilirlik sağlar.

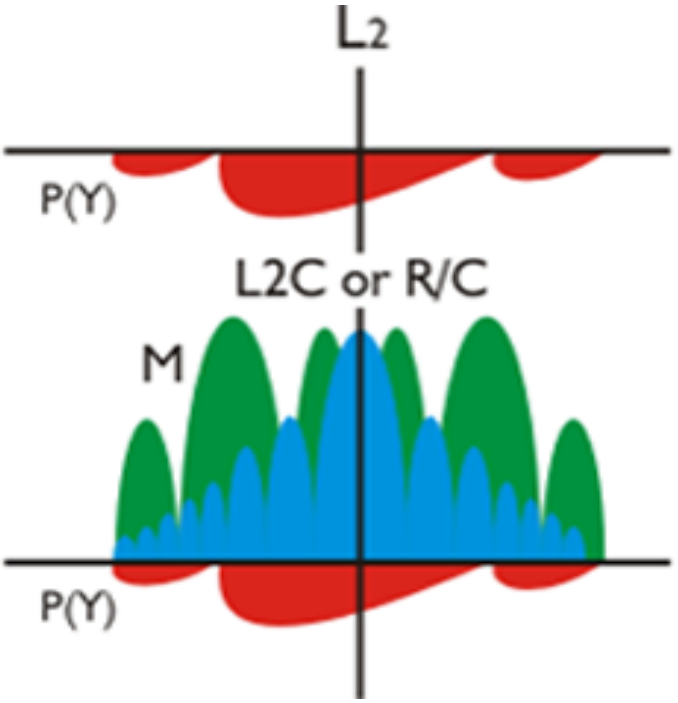
- Ekstra bant genişliği, uydu tabanlı artırma sistemlerine benzer şekilde kullanılmak üzere diferansiyel düzeltme için bir paketin dahil edilmesini sağlar ve L1 NAV saat verilerini düzeltmek için kullanılabilir.
- Her pakette, uydu verilerine güvenilememesi durumunda ayarlanacak bir uyarı bayrağı bulunmaktadır. Bu, kullanıcıların bir uydunun artık kullanılamaz durumda olup olmadığını 6 saniye içinde öğrenecekleri anlamına gelir. Böyle hızlı bir bildirim havacılık gibi can güvenliği uygulamaları için önemlidir.
- Son olarak, sistem L1 NAV mesajındaki 32 uyduya kıyasla 63 uyduyu destekleyecek şekilde tasarlanmıştır.



Şekil 2.18 CNAV Mesajı [2]

L2C FREKANS BILGILERI

İki sivil frekansın iletilmesinin ani bir etkisi, sivil alıcıların artık iyonosferik hatayı çift frekanslı P(Y)-kodlu alıcılarla aynı şekilde doğrudan ölçebilmesidir. Bununla birlikte, eğer bir kullanıcı sadece L2C sinyalini kullanıyorsa, L1 sinyaline kıyasla %65 daha fazla konum belirsizliği bekleyebilir. IS-GPS-200D'de tanımlanmıştır



Şekil 2.19 GPS L2C Sinyalleri Spekturumu [2]

2.5.44. L5 Sivil GPS L5 sinyali ilk Block IIF uydularının fırlatmasıyla (2009) kullanıma sunulmuştur. L5 frekansı üzerinde iki PRN aralık kodu iletilir: faz içi kod (I5-kodu olarak gösterilir) ve karesel faz kodu (Q5-kodu olarak gösterilir). Her iki kod da 10.230 bit uzunluğundadır ve 10,23 MHz'de (1 ms tekrarlama) iletilir. Ek olarak, I5 akışı, 1 kHz'de saatlenen 10 bitlik bir Neuman-Hofman kodu ile modüle edilirken, Q5 kodu yine 1 kHz'de saatlenen 20 bitlik bir Neuman-Hofman kodu ile modüle edilir.

GPS L5 Sinyali Özellikleri:

- Gelişmiş performans için sinyal yapısını iyileştirir

- L1/L2 sinyalinden daha yüksek iletim gücü (3db veya iki kat daha güçlü)
- Daha geniş bant genişliği 10 kat işleme kazancı sağlar
- Daha uzun yayılma kodları (C/A'dan 10 kat daha uzun)
- Havacılık Radyonavigasyon Hizmetleri bandını kullanır

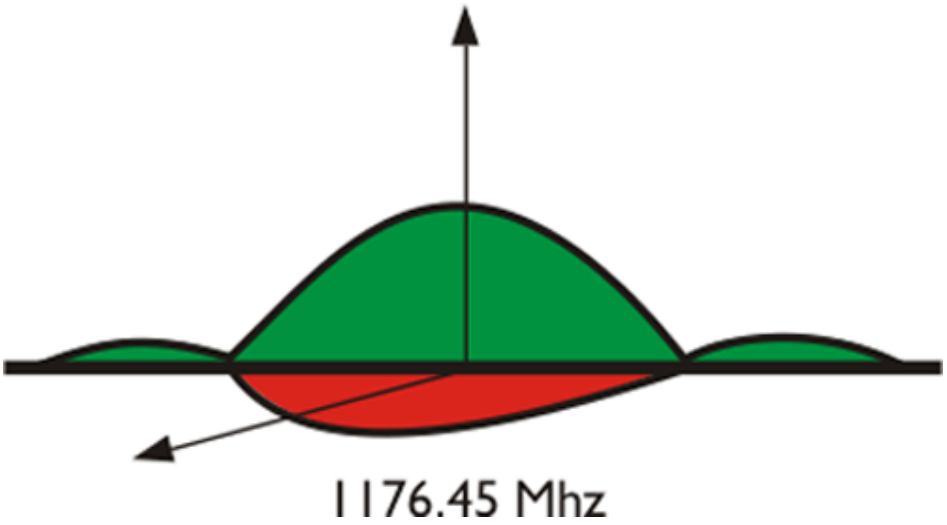
Yakın zamanda fırlatılan GPS IIR-M7 uydusu bu sinyalin bir gösterimini iletmektedir.

L5 NAVIGASYON MESAJI

L5 CNAV verileri, Uydu (SV) efemeridlerini, sistem zamanını, SV saat davranış verilerini, durum mesajlarını ve zaman bilgilerini içerir. 50 bit/s veri, 1/2 oranlı konvolüsyon kodlayıcıda kodlanır. Elde edilen saniyede 100 sembol (sps) sembol akışı yalnızca I5 koduna modulo-2 eklenir. Sonuç olarak elde edilen bit dizisi, L5 faz içi (I5) taşıyıcıyı modüle etmek için kullanılır. Bu birleşik sinyal, L5 Veri sinyali olarak adlandırılır. L5 karesel fazlı (Q5) taşıyıcıda veri yoktur ve L5 Pilot sinyali olarak adlandırılır.

L5 FREKANS BILGILERI

Havacılık navigasyon bandı olan L5 frekansında (1176,45 MHz, 10,23 MHz × 115) yayın yapılır. Hem WRC-2000 hem de IS-GPS-705, bu havacılık bandına uzay sinyali bileşeni eklemiştir. Bu sayede, havacılık topluluğu L5'e olan paraziti L2'den daha etkili bir şekilde yönetebilir.



Şekil 2.20 GPS L5 Sinyalleri Spekturumu [2]

2.5.45. L1C L1 frekansında (1575,42 MHz) yayınlanan sivil kullanım sinyali, tüm mevcut GPS kullanıcıları tarafından kullanılmaktadır. Ancak, L1C adı verilen bu yeni sinyal, 2013 için planlanmış ilk Blok III fırlatmasıyla birlikte kullanıma sunulmuştur. Taslak IS-GPS-800 spesifikasyonuna göre, L1C, Japonya'nın Quasi-Zenith Uydu Sistemi (QZSS) için temel sinyal formatı olarak geliştirilmiştir.

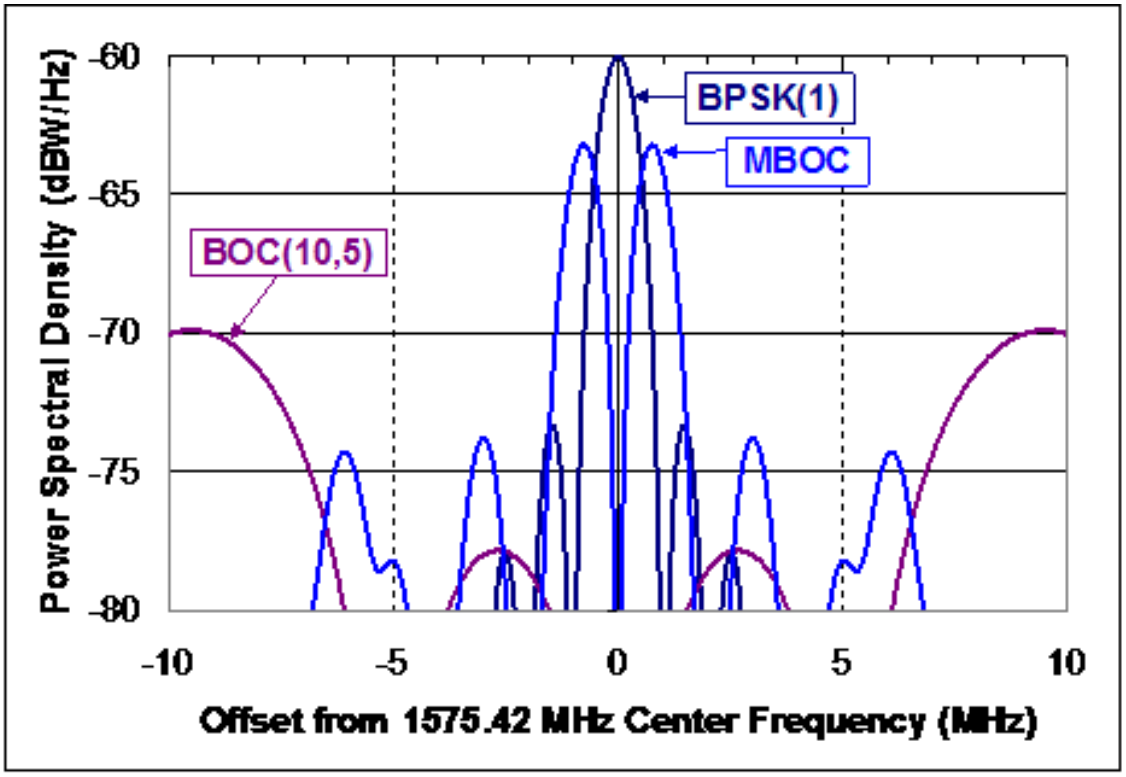
PRN kodları 10.230 bit uzunluğundadır ve 1,023 MHz'de iletilir. L2C gibi hem Pilot hem de Veri taşıyıcılarını kullanır.

Temmuz 2007 itibariyle modülasyon tekniği kesinleşmiştir. Seçilen yöntem veri sinyali için BOC(1,1) ve pilot için TMBOC kullanmaktadır. Zaman Çoğullamalı İkili Ofset Taşıyıcı (TMBOC), BOC(6,1)'e geçtiğinde 33 çevrimin 4'ü hariç tümü için BOC(1,1)'dir. Toplam L1C sinyal gücünün %25'i veriye ve %75'i pilota tahsis edilir.

GPS L1C Sinyali Özellikleri:

- Uygulama, geriye dönük uyumluluğu sağlamak için C/A kodu sağlayacaktır
- Herhangi bir gürültü tabanı artışını azaltmak için minimum C/A kod gücünde 1,5 dB artış sağlanmıştır

- Verisiz sinyal bileşeni pilot taşıyıcı takibi iyileştirir
- Galileo L1 ile daha fazla sivil birlikte çalışabilirlik sağlar



Şekil 2.21 GPS L1C Sinyalleri Spekturumu [2]

2.6 USRP

Evrensel Yazılım Tanımlı Radyo Birimi (Universal Software Radio Peripheral, USRP), yazılım tabanlı bir radyo periferik cihazıdır ve esnek bir şekilde programlanabilir radyo frekansı (Radio Frequency, RF) uygulamalarının geliştirilmesine imkan tanır. USRP, GNU Radio gibi açık kaynaklı yazılım tabanlı radyo frekansı platformlarıyla birlikte kullanılarak, geniş bir frekans aralığında (DC ila 6 GHz veya daha fazla) çalışabilir ve çeşitli kablosuz iletişim standartlarını destekleyebilir. Modüler tasarımı sayesinde, farklı RF ön uçları, veri dönüştürücüler ve dijital işlem birimleriyle uyumlu olacak şekilde yapılandırılabilir. USRP, araştırmacıların, öğrencilerin ve endüstri profesyonellerinin prototipler oluşturmasını, algoritmaları test etmesini ve gerçek zamanlı veri işleme uygulamaları geliştirmesini sağlar.

Ayrıca, genişletilebilir yapısı ve açık kaynaklı yazılım ekosistemi, yeni kablosuz iletişim protokolleri ve güvenlik çözümleri üzerinde araştırma yapmak isteyenler için ideal bir platform sunar.

Şekil 2.22 Örnek USRP Resimleri [3]

3 GPS KARIŞTIRMA/ALDATMA VE KARŞI TEDBİR YÖNTEMLERİ

3.1 Karıştırma ve Aldatma Yöntemleri

GPS karıştırma ve aldatma saldırıları, GPS sinyallerini bozan veya yanıltıcı bilgilerle manipüle eden kötü niyetli girişimlerdir. Karıştırma saldırıları, GPS alıcılarının sinyal güvenilirliğini azaltmak için sinyallerin gücünü zayıflatır veya bozar. Bu tür saldırılar, yüksek güçlü radyo frekansı (RF) sinyalleri göndererek veya yüksek güçlü radyo frekansı parazitleri yayarak gerçekleştirilebilir. Öte yandan, aldatma saldırıları, GPS alıcılarını yanıltmak için sahte sinyaller göndererek gerçekleştirilir. Saldırganlar, sahte GPS sinyalleri üretmek için zamanlama ve konum bilgilerini taklit edebilirler. Bu tür saldırılar, araçların, gemilerin veya uçakların yanlış konumlara yönlendirilmesi gibi ciddi sonuçlara yol açabilir.

Çoğu alıcı için, alınan sinyal genellikle zayıf olduğundan ve uydu sinyallerinin alınması ve izlenmesi genellikle yayılan kod korelasyonu ile belirlenir. Ancak, gerçek yaşam koşullarında, çok yollu etkiler ve yüksek güçlü elektromanyetik dalgalar alıcının normal sinyal alımını etkileyebilir. Çok yollu sinyaller genellikle gerçek sinyallerden daha düşük güce sahiptir, bu nedenle alıcı, yanlışlıkla bu sinyalleri gürültü olarak algılayabilir ve bu durumda, çok yollu etkiye direnme amacıyla daha yüksek güce sahip sinyali takip etmeye yönelebilir. Bir aldatıcı, alıcı mekanizmasını kullanarak sahtekarlık sinyalinin gücünü gerçek sinyal gücünden biraz daha yüksek bir seviyeye ayarlar. Bu, alıcıyı yanıltmak için yapılan bir harekettir, çünkü alıcı, sahtekarlık sinyalini gerçek sinyal olarak algılayabilir ve bu yanıltıcı sinyali izleyebilir.

Mevcut sahtecilik stratejileri temel olarak dört kategoriye ayrılmaktadır: sinyal yeniden oynatma GPS aldatma saldırısı , sinyal üretimi GPS aldatma saldırısı , tahmin GPS aldatma saldırısı ve gelişmiş GPS aldatma saldırısı. Tablo 3.1'de aldatma yöntemlerinin sınıflandırılmasından detaylı olarak bahsedilmiştir.

Tablo 3.1 Aldatma Yöntemlerinin Sınıflandırılması

Saldırı Tipi	**Uygulanabilirlik**	**Saldırı Etkisi**	**Yöntem**
Yeniden Oynatma Saldırısı [5], [9], [10], [11],	Kolay	Orta	Aldatıcılık yapan taraf, alınan sinyalin alıcıya iletimini geciktirerek alıcıyı yanıltır. Bu tür aldatıcılığın uygulanması nispeten basittir. Ancak, aldatıcılık yoluyla başarı oranını artırmak isteyen kişi, aldatıcılık sinyalinin parametrelerini uygun şekilde ayarlamalı ve daha etkili bir aldatıcılık sonucu sağlamak için gerekli aldatıcılık ortamını oluşturmalıdır.
Sinyal Üretimi Saldırısı [12–16], [17]	Orta	Orta-İyi	Bu aldatma yöntemi, aldatıcı sinyal üreterek sinyalin ilgili parametrelerini ayarlar, böylece alıcıların konum sonucunu kontrol etmesini sağlar.
Tahmin Saldırısı [4], [9], [18]	Orta-Yüksek	İyi	Bu aldatıcı taktik, alıcılara manipüle edilmiş konum, hız ve zamanlama verileri sağlayarak GPS tabanlı sistemlerin güvenilirliğini zayıflatır. Bu yaklaşım sadece standart sivil sinyalleri etkilemekle kalmaz, aynı zamanda bilinmeyen güvenlik kodlarına sahip bazı sivil uydu sinyallerini aldatır
Gelişmiş Aldatma Saldırısı [4]	Yüksek	İyi	Daha karmaşık alıcılar ve karşı-tedbir yöntemleri kullanan alıcılar için, alıcı yalnızca birden fazla aldatma stratejisini benimsemekle kalmaz, aynı zamanda sinyal özelliklerini birleştirerek daha etkili bir sahtecilik sinyal formatı tasarlar, böylece alıcıyı daha doğrudan ve etkili bir şekilde aldatır.

3.1.1 Sinyal Yeniden Oynatma GPS Aldatma Saldırısı

Bu yöntem, gerçek GPS sinyallerinin kaydedilmesini ve daha sonra GPS alıcılarını aldatmak için küçük değişikliklerle yeniden oynatılmasını içerir. Bu sinyallerin farklı bir konum veya zamanda tekrar oynatılmasıyla alıcı farklı bir konumda olduğuna inandırılabilir.

Temel olarak sinyal yeniden oynatma GPS aldatma saldırısı doğrudan tekrarlama, yüksek güçlü tekrarlama, seçici gecikmeli ve çok antenli alıcı olarak ayrılır.

Aldatıcı bir sinyal yeniden oynatma saldırısı başlattığında, gerçek uydu sinyalini yapay olarak doğrudan alıcıya gönderebilir, buna doğrudan yeniden oynatma sahteciliği girişimi denir. Aldatıcı, uydu sinyalinin genliğini yapay olarak artırır, buna yüksek güçlü yeniden oynatma saldırısı denir. Seçici gecikmeli yeniden oynatma saldırısı, uydu sinyalinin yayılma gecikmesine belirli bir gecikme ekler. Çok antenli alıcı tekrar saldırısı, bir aldatıcı'nın birden fazla anten kullanarak yeniden oynatma aldatma saldırısı yapmasıdır. Aldatma saldırısının sinyalleri tek bir yönden geldiğinden, aldatıcı çok antenli alıcıyı kullanarak aldatma sinyalini tekrar oynatabilir ve alıcının sinyal varış tespiti yöntemini kullanarak aldatma saldırısını tespit etmesini önleyebilir. Bu dört aldatma uygulamasının özellikleri Tablo 3.2'de gösterilmektedir.

3.1.2 Sinyal Üretimi GPS Aldatma Saldırısı

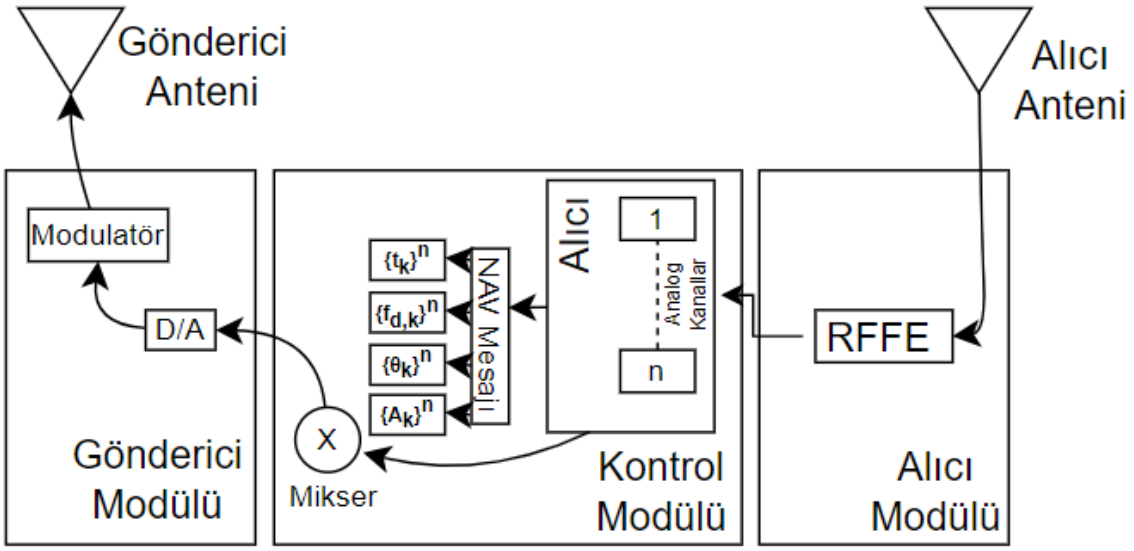
Bu yöntemde, aldatıcı sıfırdan sahte GPS sinyalleri üretir. Bu sinyaller gerçek GPS sinyallerinin özelliklerini taklit eder ancak yanlış konum, hız ve zamanlama bilgileri sağlar. Sinyal Üretimi'nin basit sinyal üretim modeli üç bölümden oluşmaktadır: uydu sinyali alma modülü, aldatma sinyali üretme modülü ve aldatma sinyali yayınlama modülü. Uydu sinyali alma modülünde, aldatma alıcısı anten aracılığıyla gerçek uydu sinyalini alır ve ardından sinyali radyo frekansı ön ucu (radio frequency front end, RFFE) aracılığıyla aldatma sinyali üreten modülün alıcısına iletir. Buna ek olarak, aldatma alıcısı sahte hedefin konumunu ve hızını elde etmek için sahte hedefi gerçek zamanlı olarak izler. Sahte sinyal üretim modülünde iki durum söz konusudur. İlk durumda, alıcı doğrudan uydu sinyalleri üretir. Bu Tablo 3.3'te bahsedilen doğrudan sinyal üretim sahteciliğidir, ancak bu durumda üretilen uydu sinyalleri gerçek sinyallerden sapma eğilimindedir. İkinci durumda, gerçek sinyale benzer bir sinyal üretmek için, aldatıcının alınan sinyali frekansa dönüştürmesi gerekir. Aldatıcı, demodülasyondan sonra temel bant sinyalini elde edecek, böylece analiz için gerçek

Tablo 3.2 Yeniden Oynatma GPS Aldatma Saldırısı Uygulamaları

Yöntem	**Uygulanabilirlik**	**Saldırı Etkisi**	**Uygulama**
Doğrudan Yeniden Oynatma [5], [10]	Kolay	Zayıf	Bu uygulama, sinyal tekrarlayıcılara benzer şekilde işlev görür; aldığı sinyali doğrudan ileterek alıcının konum sonucunu etkiler. Ancak, bu tür bir aldatma genellikle sınırlı etkililik nedeniyle tercih edilmez.
Yüksek Güçlü Yeniden Oynatma Saldırısı [5], [11]	Kolay - Orta	Orta	Bu uygulama, sahtecilik sinyalinin gücünü yapay olarak artırarak alıcıyı gerçek bir sinyal olarak algılamasını sağlamakta ve zayıf uydu sinyalini çokluyollar (multipath) etkisine bağlamaktadır. Sonuç olarak, alıcı sahtecilik sinyalini kabul etmeye ikna edilmektedir. Bu yaklaşım genellikle aldatmanın etkililiğini artırmak için diğer stratejilerle birlikte kullanılır.
Seçici Gecikmeli Yeniden Oynatma Saldırısı [9], [11]	Kolay-Orta	Orta	Aldatma uygulaması uydu sinyaline yapay bir gecikme ekleyerek yayılma kodunun fazını etkiler ve alıcının sinyali doğru bir şekilde yakalama yeteneğini bozar. Bu yaklaşım genellikle aldatmanın başarı oranını artırmak için diğer taktiklerle birlikte kullanılır.
Çoklu anten alıcı Yeniden Oynatma Saldırısı [9]	Zor	Orta-İyi	Çok antenli bir alıcı için, her anten tarafından varış açısı algılanabilir. Ancak, aldatma sinyali yüzeydeki tek bir vericiden iletilirken, antenler tarafından ölçülen yönlendirme açıları neredeyse aynıdır, bu da sahtecilik sinyalinin kolayca tespit edilmesini sağlar. Dolayısıyla, çok antenli bir alıcı, koordineli sahtecilik için birden fazla aldatma kaynağı gerektirir ve yukarıdaki aldatma uygulamalarını birleştirerek aldatma girişiminin etkinliğini artırır.

uydu sinyalinin ilgili parametrelerini elde edecek ve bir aldatma sinyali üretecektir. İkinci durumdaki sahtecilik süreci Tablo 3.3'de bahsedilen analizli sinyal üretim aldatmasıdır.

Şekil 3.1'de gösterildiği gibi, alıcı temel bant sinyalini işleyerek ve hesaplayarak dört parametre elde eder, burada $\{t_k\}^n$ alıcı kanal $1 \sim n$'in k'ıncı C/A kod periyodunun tahmin



Şekil 3.1 Sinyal Üretimi ile Aldatma

başlangıç anıdır. $\{\phi_k\}^n$, $\{t_k\}^n$' deki alıcı kanal 1 $\sim$ *n*'in tahmin taşıyıcı fazı.$\{f_{d,k}\}^n$, $\{t_k\}^n$' deki alıcı kanal 1 $\sim$ *n*'nin tahmini doppler frekans kayması ve $\{A_k\}^n$, $\{t_k\}^n$' deki alıcı kanal 1 $\sim$ *n*'nin sinyal genliğidir. Sahtekarlık başarı oranını artırmak için, sahtekar genellikle yukarıda bahsedilen inkar ortamı sahtekarlığı olan sahtekarlık sinyalinin $\{A_k\}^n$ genliğini artırır. Sahtekarlık alıcısı tarafından hesaplanan parametreler kontrol modülüne girilir. Kontrol modülünden sonraki sahtecilik sinyali, sahtecilik hedef alıcısının tüm yakalama ve izleme döngüsü ile tamamen senkronize edilebilir. Sahte N kanalın her birinde üretilen sinyaller, alıcı modülü tarafından izlenen sinyallere karşılık gelen kanal parametreleriyle aynıdır, böylece Tam kanal sahteciliği uygulanabilir. Yukarıda bahsedilen dört sahtecilik sahtekarlığı saldırısının spesifik özellikleri Tablo 3.3'te gösterilmektedir.

3.1.3 Tahmin GPS Aldatma Saldısı

GPS sahteciliğini önleme araçlarını içeren bazı navigasyon mesajlarında, navigasyon mesajının güvenliğini artırmak için bilinmeyen bir güvenlik kodu eklenir. Aldatıcı, navigasyon mesajındaki bu güvenlik kodunu tahmin edemez ve dolayısıyla alıcı tarafından tanınabilen bir navigasyon mesajı üretemez. Bu nedenle, sahteciliğe karşı tek başına güvenemez. Bu yüzden, aldatıcı, alınan navigasyon sinyalini tahmin etmeli ve tahmini

Tablo 3.3 Sinyal Üretim GPS Aldatma Saldırısı Uygulamaları

Yöntem	**Uygulana-bilirlik**	**Saldırı Etkisi**	**Uygulama**
Doğrudan Sinyal Üretim Saldırısı [13]	Orta	Orta	Aldatıcı, çeşitli uydu navigasyon arayüz dosyaları aracılığıyla hızlı ve akıllı işlemci teknolojilerini kullanarak doğrudan uydu sinyalleri üretir. Ancak, bu şekilde üretilen uydu sinyalleri, mevcut yayılan uydu sinyalinin faz farkı ve ilgili parametreleri ile uyumlu değildir ve bu nedenle alıcı tarafından güvenilir bir şekilde alınmaları zordur.
Analizli Sinyal Üretimi Saldırısı [17]	Orta-Zor	Orta-İyi	Aldatma sinyali vericisi, bir alıcı ve bir vericiden oluşur. Alıcı, alınan gerçek uydu sinyalini analiz eder ve ardından elde edilen sinyal parametrelerini hemen iletilen aldatma sinyaline dahil eder, böylece aldatma başarı oranını artırır.
İnkar Ortamlı Sinyal Üretim Saldırısı [14], [15]	Orta	Orta	Sinyal aldatma başarı oranını artırmak amacıyla, aldatıcı alıcıya gps karıştırma sinyali ile müdahale gönderir, bu da alıcının karışmasına ve böylece mevcut izleme hassasiyetinin kaybolmasına neden olur. Sonuç olarak, aldatıcı, bu durumlarda aldatma sinyalini iletmekte ve böylece alıcının daha kolay almasını sağlamaktadır, bu da aldatma amacını gerçekleştirmektedir.
Tam Kanal Sinyal Üretim Saldırısı [12], [16]	Zor	İyi	Tam kanal aldatma, bilinen tüm kanalların (veya hedef alıcının alabileceği kanalların) kapsamlı bir şekilde aldatılmasını içerir. Bu, aldatıcının aynı anda birden fazla uydu sinyalini aldatması gerektiği anlamına gelir. Sonuç olarak, aldatıcı alıcının konum sonucunu daha hassas bir şekilde kontrol eder.

sonuca göre navigasyon mesajının içeriğini değerlendirmelidir. Günümüzde, iki tür ESA bulunmaktadır: Güvenlik kodu tahmini ve tekrar oynatma (security code estimation and replay, SCER) ve ileri tahmin saldırısı (forward estimation attack, FEA). Güvenlik kodunu içeren navigasyon mesajı, gönderici tarafından bir şifreleme algoritması kullanılarak oluşturulur. Aldatıcının menzil kodunun kod ofsetini tahmin etmesi ve taşıyıcı fazını tahmin etmesi gerekir. Aldatıcı, güvenlik kodlarını başarıyla tahmin ettikten sonra sahtekarlık sinyalleri üretmek için gerçek uydu sinyal parametrelerini kullanır ve aynı zamanda yayılma kodlarını ve taşıyıcı kopyalarını günceller.

Aldatıcı güvenlik kodu tahmini ve tekrar oynatma saldırısı başlatmak istiyorsa navigasyon mesajları, navigasyon sinyalleri ve sinyal tahmin yöntemleri gibi çeşitli yönleri incelemelidir. Bu sahtecilik saldırısı için en önemlisi güvenlik kodunun doğru tahmin edilmesi ve yapay olarak eklenen gecikmenin hassas bir şekilde kontrol edilmesidir. Mevcut SCER karşı tedbir yöntemi için, alıcı esas olarak sinyal olasılık analizi perspektifinden olasılık karar fonksiyonunu oluşturur ve alıcı ayrıca sinyal gücü, gecikme ve bilgi bütünlüğünü birleştirerek sahtecilik saldırısını değerlendirir. Ancak, bu sahtecilik yöntemi zordur ve genellikle gerçek projelerde kullanılmaz.

FEA saldırısı son yıllarda önerilen bir ön tahmin yöntemidir. Çoğu alıcı kod çözmeden önce navigasyon mesajını kontrol etmediğinden, aldatıcı alıcıyı aldatmak için önceki bilgilerle birlikte bir navigasyon mesajı oluşturabilir. FEA saldırısındaki navigasyon mesajı genellikle kimlik doğrulama işlevine sahip bir navigasyon mesajıdır. Navigasyon mesajının içsel uygunluğuna göre, navigasyon mesajı bilgisi aldatıcı tarafından ne kadar çok elde edilirse, aldatıcı tarafından tahmin edilen yanlış navigasyon mesajı o kadar doğru olur. FEA'da, aldatıcı sahtekarlık sürecini uygulamak için gerçek bilgi gönderilmeden önce bile sahte bilgi gönderebilir. Buna karşın, SCER'in sahtekarlık işlemini gerçekleştirebilmesi için önce gerçek sinyali elde etmesi ve ardından sinyal parametrelerini tahmin etmesi gerekir.

Her iki saldırı türü de sinyal tahminine dayanmaktadır. Bu iki saldırının uygulanması zor olduğundan, aldatıcı genellikle bunu benimsemez. Ancak, gönderici gelecekte bazı kriptografi tabanlı sahteciliğe karşı yöntemleri benimserse, bu iki saldırının aldatma etkisi

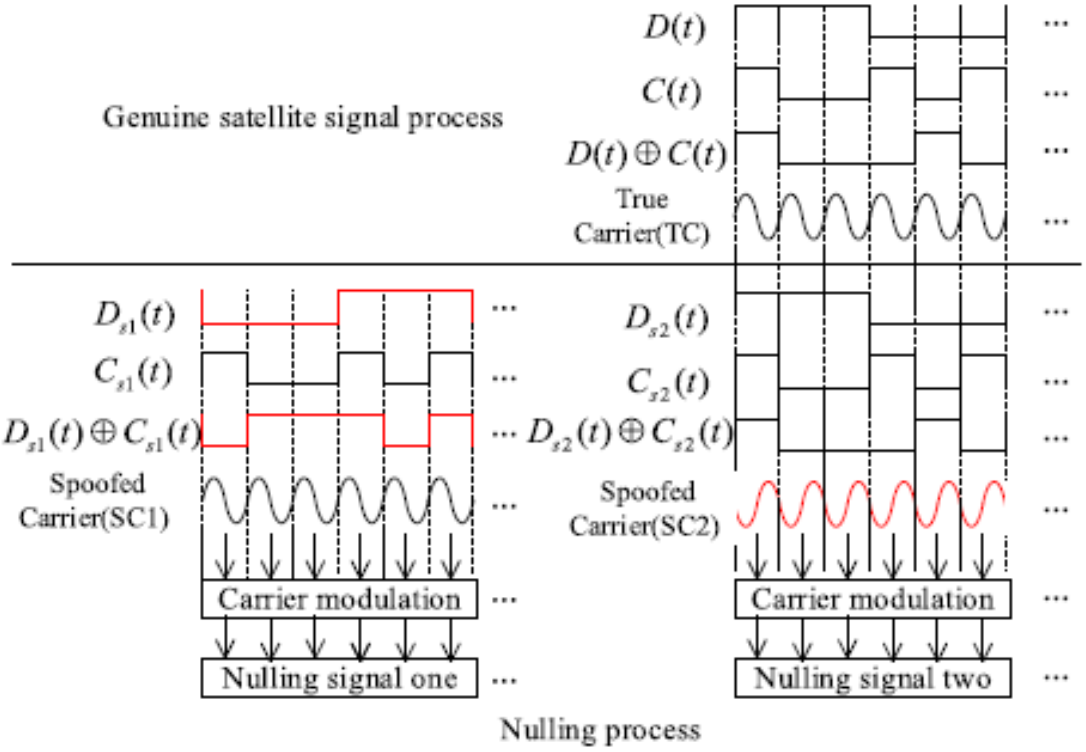
de bir miktar etkili olacaktır. Bu nedenle, kriptografik tabanlı sahteciliği önleme yöntemleri tasarlanırken, alıcının bu iki saldırının direncini göz önünde bulundurması gerekir.

3.1.4 Gelişmiş Aldatma Saldırısı

Yukarıdaki sahtekarlık saldırısı türlerine ek olarak, bazı akademisyenler son yıllarda iptal etme (nulling) saldırısı ve işbirlikçi girişim saldırıları dahil olmak üzere başka aldatma saldırıları da önermişlerdir. GPS karıştırma ile sahtekarlık tekniklerinin birleştirilmesi sahtekarlık saldırılarının etkinliğini artırabilir. Karıştırma gerçek GPS sinyallerini bozarak sahte sinyallerin GPS alıcılarını tespit edilmeden aldatmasını kolaylaştırır.

Nulling'in bir GPS sahtekarlığı yöntemi olarak nasıl kullanılabileceği aşağıda açıklanmıştır:

Sinyal Bastırma: Saldırgan önce uydulardan iletilen gerçek GPS sinyallerini tespit eder. Daha sonra hedeflenen bir alanda bu gerçek sinyalleri etkisiz hale getirmek veya bastırmak için özel ekipman veya yazılım tanımlı telsizler kullanırlar. Bu etkisizleştirme işlemi, çevredeki GPS alıcıları tarafından meşru GPS sinyallerinin alınmasını etkili bir şekilde engeller. Sahte Sinyal Üretimi: Gerçek GPS sinyallerini bastırırken, saldırgan aynı anda tahrif edilmiş konumlandırma bilgileri içeren sahte GPS sinyalleri yayınlar. Bu sahte sinyaller gerçek GPS sinyallerini taklit etmek için tasarlanmıştır ancak yanlış konum verileri sağlar. Saldırgan bu sahte sinyalleri bir GPS sinyal üreteci kullanarak veya yazılım tanımlı radyoları sahte GPS sinyalleri iletecek şekilde programlayarak üretebilir. Aldatıcı Navigasyon: Nulling ve Aldatma bölgesi içindeki GPS alıcıları yanlışlıkla saldırgan tarafından iletilen sahte sinyallere kilitlenir. Sonuç olarak, sahte GPS verilerine dayanarak hatalı konum, hız ve zamanlama bilgileri hesaplarlar. Saldırının Gizlenmesi: GPS alıcıları gerçek sinyallerin yokluğunda herhangi bir anormallik tespit edemeyebileceğinden, gerçek GPS sinyallerinin geçersiz kılınması sahtekarlık saldırısının varlığının gizlenmesine yardımcı olur. Bu da kullanıcıların sahtekarlığa uğradıklarını fark etmelerini zorlaştırır ve saldırının etkinliğini artırır.



Şekil 3.2 İptal Etme İşlem Süreci [4]

Şekil 3.2'de görülebileceği gibi, aldatma uydu bilgisi $Ds1(1)$ gerçek bilgi $D(1)$'den farklıdır, ancak mesafe kodu ve taşıyıcı aynıdır ($C(t) = Cs1(t)$ ve gerçek taşıyıcı (TC)= Aldatma taşıyıcı (SC1)). Nulling sinyalinin iki $Ds2(1)$ ve mesafe kodu $C2(1)$ bilgileri gerçek sinyalinkiyle aynıdır, ancak taşıyıcı fazında π sapması vardır. İkinci sinyalin işlevi, alıcı tarafından alınan gerçek sinyali yok etmektir. Nulling sinyali iki, alıcının gerçek sinyali yakalamamasını, yalnızca nulling sinyali birini yakalamasını ve son olarak aldatma amacına ulaşmasını sağlar. Alıcı tarafından alınan GNSS sinyalinin ifadesi aşağıdaki gibi olabilir.

$$R(t) = Re\left\{\sum_{1}^{N} \mathrm{A}_i \mathrm{D}_i[t-\tau_i(t)\mathrm{C}_i[t-\tau_i(t)]e^{j[\mathrm{w}_c t-\phi_i(t)]}\right\} \tag{3.1}$$

burada *N*, bileşen yayma koduna özgü sinyal sayısıdır, Aj sinyalin genliğidir, Di sinyalin verisidir, Ci sinyalin PN kodudur, $ti(1)$ sinyalin kod fazıdır, ; (1) sinyalin atım taşıyıcı fazıdır. Bozma sürecinde, sinyal bir ve sinyal iki i= 1,....,*N* için aşağıdaki ilişkiyi sağlamalıdır. $Ci +$

Tablo 3.4 Gelişmiş GPS Aldatma Saldırısı Uygulamaları

Yöntem	**Uygulana-bilirlik**	**Saldırı Etkisi**	**Uygulama**
Sıfırlama Saldırısı [4]	Zor	Orta-İyi	Saldırgan, gerçek sinyalle aynı güç gecikmesini gönderir, ancak taşıyıcı fazı terstir. Alıcı bu sinyali aldıktan sonra gerçek sinyalle iptal edecek ve bu da alıcının gerçek sinyalin sinyal parametrelerini kaybetmesine ve alıcının karşı tedbir performansını düşürmesine neden olacaktır.
Ortak Girişim Saldırıları [4]	Çok Zor	İyi	Saldırı modu, yukarıda bahsedilen aldatma stratejisini kullanan birden fazla spoofer tarafından koordine edilir. Bazı alıcılar karmaşık antiAldatma yöntemleri benimsemiş olsa bile, bilgilerin bütünlüğü ve güvenilirliği garanti edilemeyebilir.

$N(t) = Ci(t)$ ve $Di + N(t) = Di(t)$. Sinyal ikinin işlevi, alıcı tarafından alınan gerçek sinyali ortadan kaldırmaktır .Bu nedenle, sıfırlama sinyali aşağıdakilere uymalıdır $A_{s[i+N]} = A_i$, $\tau_{s[i+N]}(t) = \tau_i(t)$ ve $\phi_{s[i+N]} = \phi_i(t) + \pi$.

Yayılı spektrum iletişimi düşük dinleme olasılığı özelliğine sahiptir. Bu makalenin amacı, sivil GNSS navigasyon sisteminin sahteciliğe karşı koruma ve sahtecilik teknolojisini analiz etmektir. Çoğu sivil sistemde kullanılan yayılı spektrum teknolojisi doğrudan sıralı yayılı spektrum yöntemidir (DSSS). DSSS sinyallerinin kesilme olasılığının düşük olması, herhangi bir düşman alıcısının doğrudan sıralı yayılı spektrum sinyallerini almak için yeterli bant genişliğine sahip olsa bile, aynı zamanda çok fazla gürültü gücü alacağı ve bunun da kesilen sinyalin sinyal-gürültü oranının çok düşük olmasına neden olacağı gerçeğinden kaynaklanmaktadır. Doğrudan yayılı spektrum ile karşılaştırıldığında, frekans atlamalı iletişim askeri navigasyon sinyallerinde yaygın olarak kullanılmaktadır. Frekans atlamalı sinyalin LPI sinyali olarak kullanılmasının nedeni, bir frekansı kapladığı sürenin çok kısa olması ve düşmanın sinyalin varlığını tespit etmesini zorlaştırmasıdır. Başka bir deyişle, frekans atlamalı sinyal her frekansta kısa bir süre kalır, böylece sinyalin o anda alındığı güç önemli ölçüde azalır. Nulling saldırısı ve işbirlikçi girişim saldırılarının temel özellikleri Tablo 3.4'te gösterilmektedir.

Nulling saldırısı, alıcıların sahtekarlık başarı oranını artırmak için son yıllarda önerilen

bir sahtekarlık yöntemidir. Ancak, nulling saldırısının uygulanması çok zordur. Şimdiye kadar, bu saldırı yöntemi sadece teorik bir girişim aracıdır ve uygulamaya konulmamıştır. İşbirlikçi girişim saldırıları, RAIM alıcıları gibi sahteciliğe karşı alıcıların normal çalışmasını etkilemek için tasarlanmıştır. Gelişmiş sinyal sahteciliği için, bunların çoğu teorik aşamada kalmaktadır. Bununla birlikte, donanım ve bilgisayar teknolojisinin sürekli gelişmesiyle, teorik sahtekarlık modu da gelecekte gerçeğe dönüştürülebilir. Bu nedenle, sahteciliğe karşı yöntemler tasarlanırken bu sahtecilik yöntemlerinin dikkate alınması gerekir.

3.1.5 GPS Karıştırma Yöntemleri

GPS aldatma ve karıştırma farklı teknikler olmakla birlikte, birbirleriyle bağlantılı olabilirler. Karıştırma genellikle gerçek GPS sinyallerinde bozulmalar yaratarak sahtekarlık saldırılarını kolaylaştırmak için bir araç olarak kullanılır, bu da sahte sinyallerin GPS alıcılarını tespit edilmeden aldatmasını kolaylaştırır. Saldırganlar belirli bir alandaki GPS sinyallerini bozarak sahtecilik saldırılarının etkinliğini artırabilir ve şüphelenmeyen kullanıcıların navigasyon sistemlerini manipüle edebilir.GPS karıştırma için farklı teknikler mevcuttur.

Sürekli Dalga Karıştırma: Bu yöntem GPS sinyalinin frekansında sabit bir dalga iletmeyi içerir. Esasen GPS alıcısını sürekli bir sinyalle doldurur ve gerçek GPS sinyallerini etkili bir şekilde işleyemez hale getirir.

Darbe Karıştırma: Darbe karıştırma, GPS sinyalinin frekansında kısa enerji patlamalarının iletilmesini içerir. Bu darbeler GPS sinyallerinin alımını aralıklı olarak bozarak GPS alıcılarında parazite neden olabilir.

Tarama Karıştırma: Tarama karıştırma, karıştırma sinyalinin frekansının geniş bir aralıkta hızla değiştirilmesini içerir. Bu teknik, sürekli karıştırmadan kaçınmak için frekans atlama yeteneklerine sahip olabilecek GPS alıcılarını bozmayı amaçlamaktadır.

Baraj Gürültü Karıştırma: Baraj gürültü karıştırma hedeflenen sistemin frekans bandını gürültü ile doldurarak geniş bir aralıkta geniş bir radyo frekansı spektrumunun iletilmesini içerir. GPS frekans bantları boyunca sürekli bir gürültü akışı ile doldurur ve alıcının gerçek

GPS sinyallerini karıştırma parazitinden ayırt etmesini zorlaştırır. Bu kaba kuvvet yaklaşımı alıcının bant genişliğini zorlayarak navigasyon hatalarına veya GPS kilidinin tamamen kaybolmasına neden olur.

Noktasal Karıştırma: Noktasal karıştırma tüm bandı kapsamak yerine GPS bandı içindeki belirli frekansları hedef alır. Bu yöntem, belirli GPS işlevlerini veya uygulamalarını seçici olarak bozmak ve diğerlerinin etkilenmemesine izin vermek için kullanılabilir.

Dijital Radyo Frekansı Hafızası Karıştırma Dijital Radyo Frekansı Hafızası (Digital Radio Frequency Memory , DRFM) karıştırıcıları gelen GPS sinyallerini kaydedebilen, değiştirebilen ve kasıtlı hatalarla yeniden iletebilen sofistike elektronik harp sistemleridir. Bu yöntem basit bir karıştırmadan daha ileri bir yöntemdir ve GPS alıcılarını kandırarak yanlış konumlar hesaplamalarına neden olan yanıltma saldırıları için kullanılabilir.

3.2 Literatürde Karıştırma ve Aldatma Yöntemleri

Günlük hayatımızda GPS'in vazgeçilmez bir parçası haline geldiğini görüyoruz. Uygulamaları jeodeziden ölçmeye, navigasyona, spora vb. kadar çeşitlilik göstermektedir.[19]. Tüm bu sistemler GPS verilerinin doğruluğuna bağlıdır. [20] Çok sayıda olgu GNSS'in belirli güvenlik riskleri taşıdığını ve saldırı tehdidi altında olduğunu kanıtlamaktadır. Özellikle, GNSS sivil sinyal alıcıları, GNSS sivil sinyallerinin formatı ve modülasyonu kamuya açık olduğundan, sahtekarlık saldırısı ve karıştırma saldırısına yanıt verme konusunda bazı güvenlik açıklarına sahiptir. [4]

Uydu dünyadan çok uzakta çalıştığı için alıcı tarafından alınan sinyal çok zayıftır kabaca Japonya'daki 25 Watt'lık bir ampulü Los Angeles, Kaliforniya'dan görmeye eşdeğerdir [20] ve kasıtlı parazitlerden ve kazara oluşan parazitlerden kolayca etkilenir. Uydu navigasyon sinyallerinin doğruluğu ve bütünlüğü garanti edilemez .

GPS ve uygulamaları üzerine kapsamlı çalışmalar yapılmıştır, ancak sinyal karıştırma üzerine yapılan çalışmalar hala çok azdır. Bunun nedeni GPS Sinyal Simülatörlerinin sahip olduğu yüksek maliyettir.

Idris ve arkadaşları [21]'de GPS L1 ve GPS L2 sinyallerinde radio frekans girişimi (Radio Frequency Interference, RFI) altındaki GPS alıcılardaki etkileri incelemiştir. -140dB den başlanarak veriler bozulana kadar parazit sinyali uygulanmış. Tek (Promark-3) ve iki frekanslı(Topcon Hiper-Ga) GPS alıcılar kullanılmış. Tek frekanslıalıcılar girişimden -95dBm seviyelerinde etkilenmeye başlamış çift frekanslı alıcı ise daha yüksek girişim sevilerine kadar bilgileri daha iyi alabilmiştir.[22] ' de benzer bir çalışma SDR kullanılarak yapılmıştır. GPS'in alıcıdaki tipik gücü basit bir hesaplamayla hesaplanmış ve tipik güçten yüksek bir seviyede L1 (1575,42 MHz) bandında sinyal üreterek karıştırma denemesi yapılmıştır. Çalışma sonucunda karıştırma işleminin başarılı olduğundan bahsedilmiştir

Elezi çalışmasında [20] farklı karıştırma tekniklerinin GPS sinyalleri üzerindeki etkileri incelenmiştir. İncelemeler MATLAB simulink üzerinde yapılmıştır. Şok Karıştırma (Pulse Jamming, PJ), Nokta Karıştırma (Spot Jamming, SJ), Baraj Gürültü Karıştırma (Barrage Noise Jamming, BNJ) ve Tarama Karıştırma (Sweep Jamming, SWJ) methodlarından hangisinin en yüksek karıştırma etkisi olduğu karşılaştırılmış. Karşılaştırmalar Karıştırma/Sinyal oranlarındaki Bit Hata Oranına(Bit Error Rate, BER) bakılarak yapılmıştır. Simülasyonun sonunda Spot Noise karıştırmanın en etkili karışma tekniği olduğu sonucu gözlemlenmiş.

Ferreira ve arkadaşlarının makalesinde [23] Nuand'ın programlanabilir BladeRF x40 platformu ve GNU Radio yazılım geliştirme araç seti kullanılarak, spektral verimlilik, enerji verimliliği ve karmaşıklık göz önünde bulundurularak baraj karıştırma, tarama karıştırma, ardışık darbeli karıştırma, ton karıştırma, protokol farkında karıştırma teknikleri incelenmiş ve değerlendirilmiştir. En iyi performans gösteren karıştırıcı, GPS sinyalinin vericisi tarafından kullanılana benzer bir mimari kullanan protokol farkında karıştırma olmuştur. Bu yaklaşımı kullanarak, karışan sinyal, aynı spektral davranış sergiledikleri için hedef sinyalle daha etkili bir şekilde karışır, bu sinyalin bilgisini yok eder veya başka bir şekilde alıcıda alımını neredeyse imkansız hale getirir.

Sivil GNSS Arayüz Kontrol Dokümanı (ICD), sivil uydu navigasyon sinyalleri için taşıyıcı frekansı, modülasyon modu, navigasyon mesajı vb. gibi ilgili parametrelerin ayrıntılı

açıklamalarına ve hesaplarına sahiptir. Aldatıcı, gerçek uydu navigasyon sinyalini teknik yollarla kolayca taklit edebilir ve ardından belirli bir sahtekarlık stratejisi ile alıcıya sahtekarlık sinyalleri gönderebilir. Bu tür bir sahtekarlık güçlü bir kılık değiştirmeye sahiptir ve hedef alıcının aldatıldığını zamanında anlamasını zorlaştırır. Alıcı, sahtekarların önceki varsayımlarına göre yanlış sahte menzil, konum ve zamanlama alabilir. [4].

Koordineli bir dizi yanlış konum veya zamanlama düzeltmesi, yanlış düzeltmelere inanan bir kullanıcı platformu tarafından tehlikeli davranışlara neden olabilir. [9]. Örneğin, GPS aldatma, havada asılı duran bir drone'u planlanmamış bir dalışa göndermek [24] ve bir yatı rotasından saptırmak [11] için kullanılmıştır.

2014 yılında yayınlanan bir bildiride, Tae-Hee Kim ve ekibi GPS L1 sinyali üretebilen bir donanım geliştirmişlerdir. Bu donanımı kullanarak ürettikleri GPS sinyalini, U-Blox alıcısı üzerinde gerçek GPS sinyaliyle karşılaştırmışlardır. Yapılan çalışma sonucunda, U-Blox alıcısında üretilen GPS L1 sinyalinin gerçek GPS sinyaliyle benzer navigasyon sonuçları verdiği ve GPS L1 sinyalinin bir donanım ile üretilebileceğini mümkün kılmışlardır. [10].

Humphreys ve ekibi tarafından yürütülen çalışmada [25], sivil GPS sinyal doğrulama tekniklerinin geliştirilmesi ve değerlendirilmesi için Texas Aldatma Test Battery (TEXBAT) adlı bir veri seti tanıtılmıştır. TEXBAT, sivil GPS alıcılarının aldatma direncini tanımlayan bir standart taslağı olarak da düşünülebilir ve kaydedilen senaryoların canlı saldırıların sadık bir temsili olmasını sağlamak üzere tasarlanmıştır. TEXBAT'in kayıt kurulumu, mümkün olduğunca karşılık gelen canlı saldırıların sadık bir temsili olmasını sağlamak amacıyla yapılmıştır. Bu veri seti, GPS aldatma konusunda önemli bir araç olarak kullanılmaktadır ve sinyal üretimi ile GPS aldatma saldırılarına temel oluşturmaktadır.

Jafarnia ve diğerleri tarafından yapılan çalışmada [26], GPS aldatmaya karşı dayanıklılık, aldatma teknikleri ve karşı yöntemler kapsamlı bir şekilde incelenmiştir. Özellikle, sivil araçların GPS sinyallerine olan bağımlılığı ve bu sinyallere karşı dayanıklılığın önemi vurgulanmıştır. GPS aldatma saldırısı altındaki bir alıcının maruz kaldığı sinyal modelleri detaylı olarak ele alınmış ve bu modellerin formülasyonları incelenmiştir. Ayrıca, GPS aldatma yöntemlerine karşı alınabilecek tedbirler ve alıcı üzerinde algılanabilmesi için

öneriler sunulmuştur. Çalışmada, farklı durumlar için test edilebilecek üç farklı senaryo önerilmiş ve bu senaryolar için modellemeler yapılmıştır. Bu analizler, GPS aldatma saldırılarına karşı savunma stratejilerinin geliştirilmesi için önemli bir temel oluşturmaktadır.

Psiakis'in çalışmasında [9], GPS aldatma yöntemlerinin, GPS sinyallerinin doğruluğunu teyit eden RAIM gibi mekanizmaların etkinliğini zorladığı belirtilmektedir. Aldatma genellikle iki ana yöntemle gerçekleştirilir. İlk yöntemde, alıcıya önce bir jamming uygulanır ve ardından daha güçlü bir aldatma sinyali yayılır. İkinci yöntemde ise gerçek GPS sinyalinin parametreleri takip edilerek, aldatma sinyali yavaşça güçlendirilir ve alıcının bu sinyale kilitlenmesi sağlanır. Askeri sistemlerde, kriptolu sinyalleri aldatmak için meaconing ve estimate-and-replay saldırıları kullanılır; bu yöntemler sinyalleri kaydedip yeniden yayarak çalışır. Nulling gibi yöntemler de kullanılabilir, ancak bu yöntemlerin başarılı olabilmesi için gerçek sinyalin faz ve genlik değerlerinin doğru şekilde bilinmesi gerekmektedir. Aldatma sinyallerinin fark edilmemesi için büyük farklılıklar yaratmaması önem taşır.

Sahte sinyal saldırılarını başarılı bir şekilde gerçekleştirebilmek için sahte sinyalci tipi, işletme konumu, sahte sinyal etkisi, sahte sinyal teknikleri ve çeşitli uygulamalar için gizli GPS aldatma stratejileri hakkında kapsamlı bir anlayış gerekmektedir. [18], çeşitli uygulamalar için gizli GPS aldatma için dört yeni aldatma tekniği (sürekli yanıltıcı hedef, sürekli yürüyen hedef, sürekli kaçırma hedefi ve sürekli yürüyen kaçırma hedefi modelleri) ve bunların matematiksel gerçekleştirilmesini önermektedir. Ayrıca, çeşitli sivil ve askeri uygulamalar için etkili aldatma stratejileri (statik kaçırma, dinamik kaçırma, yürüme pozisyonu ve sabit pozisyon) sunmaktadır. Dahası, yat, uçak, kamyon, tren, güvenlik etiketli suçlular ve cep telefonları gibi çeşitli hedef tipleri ve bunların GPS aldatma zafiyetleri de dahil edilmiştir.

GPS aldatma tekniklerinin modellenmesi ve karakterizasyonu, siber güvenlik açısından önemli bir araştırma alanıdır. Bu çalışmalar, aldatma saldırılarına karşı etkili savunma mekanizmaları geliştirmek için temel oluşturur. Van et al. tarafından yapılan bir çalışmada [27], aldatma teknikleri katmanlı olarak modellenmiştir. Bu modelleme, dağıtım mimarilerini, sinyal oluşturmayı, konum değiştirme stratejilerini, zaman ve bilgi değiştirme

stratejilerini ve uygulama ve ağ düzeyi saldırılarını içerir. Larcom ve diğerleri [28]'de ise GPS sinyallerinin işlevini ve GPS aldatmanın ne olduğunu tanımlar. Bu çalışma, GPS aldatma durumlarında olası olayları ve farklı senaryoları simüle edebilmek için bir simülasyon yaklaşımı önerir. GPS aldatma tekniklerinin modellenmesi ve bu tekniklere karşı savunma mekanizmalarının geliştirilmesi, GPS sistemlerinin güvenliğini sağlamak için önemli bir adımdır.

[12–16] çalışmaları, düşük maliyetli yazılım tanımlı radyo (SDR) platformları ve açık kaynaklı yazılım kütüphaneleri (GPS-SDR-SIM, GNSS-SDR) kullanılarak gerçekleştirilen GPS sahteciliği ve karartma saldırılarını detaylı bir şekilde incelemektedir. Songala ve ekibi, GPS-SDR-SIM ve HackRF One gibi araçlarla basit bir sahteciliğin nasıl gerçekleştirilebileceğini göstermiştir. Margana ve meslektaşları, özellikle dronların yetkisiz kullanımını engellemek için GPS sahteciliğinin önemini vurgulamış ve iç ve dış ortamlarda gerçekleştirdikleri başarılı sahtecilik deneylerini rapor etmişlerdir. Saputro ve ekibi, BladeRF X40 ve GNSS-SDR yazılımı gibi araçlar kullanarak dronlara özellikle DJI Phantom 3 Standard dronuna yönelik GPS karartma ve sahteciliği saldırılarını detaylı bir şekilde incelemişler ve iç ve dış mekanlarda yapılan deneylerinde başarılı sonuçlar elde etmişlerdir. Nguyen ve arkadaşları, SDR tabanlı bir GPS alıcısı ve GPS sahteciliği vericisi tasarlayarak dinamik konum izlemesi ile GPS sahteciliği saldırılarını incelerken, Gaspar ve meslektaşları ile Viet ve ekibi, SDR platformları ve GPS sinyal simülasyonları kullanarak İHA'lara yönelik sahtecilik ve karartma müdahalelerini araştırmışlardır. Bu çalışmalar, Sinyal yeniden oynatma GPS saldırıları ve sinyal üretimi GPS saldırılarının gerçek hayattaki kullanımlarına dair örnekler sunmaktadır. Ayrıca bu çalışmalar, düşük maliyetli SDR sistemlerinin ve açık kaynaklı yazılımların kullanılmasıyla GPS sinyallerinin manipülasyonunun potansiyel tehlikelerini ve bu tür saldırılara karşı savunma stratejilerini detaylı bir şekilde ele almaktadır.

Viet yaptığı çalışmada [17] MATLAB simulinkte GPS sinyali üretilmiş. Bu makalede, dijital ara frekans (IF) GPS sinyali simülasyon modeli sunulmaktadır. Bu tasarım, dijitalleştirilmiş IF GPS sinyalini temsil eden matematiksel bir model üzerine geliştirilmiştir. Detaylarında, C/A kodu, navigasyon verileri ve P kodu ve gürültü modelleri aynı anda bazı başlangıç ayarları ile yapılandırılmıştır. Simülasyon sonuçları, simüle edilen sinyallerin gerçek

sinyallerle aynı özellikleri paylaştığını göstermektedir (örneğin, C/A kodu korelasyon özellikleri ve geniş spektrum). Simüle edilen GPS IF sinyal verileri, GPS alıcılarının çeşitli sinyal işleme algoritmaları için giriş olarak çalışabilir, örneğin, edinme, izleme, taşıyıcı-gürültü oranı (C/No) tahmini ve GPS sahteciliği sinyali oluşturma. Özellikle, simüle edilen GPS sinyali, simülasyon sırasında gürültü üreticisinin S/N oranı değerlerini ayarlayarak senaryoları gerçekleştirebilir (örneğin, sinyal kesintileri, GPS sinyal gücünde ani değişiklikler), bu da drone güvenliği uygulamaları için İHA'lara sahtecilik/karartma müdahalelerinin kurulum deneyleri olarak kullanılabilir.

3.3 GPS Aldatma Karşı Tedbir Yöntemleri

Sahtekarlık saldırılarının tespiti ve bastırılması üzerine bir çok kapsamlı araştırma yürütülmektedir. Aldatma saldırıları genellikle uydu sinyalinin bastırılmaması durumunda tespit edilebilir. Aldatma tespiti, alınan sinyalden sahte sinyal ile gerçek uydu sinyalini ayırt etmeyi amaçlar. Sahte sinyaller navigasyon ve konumlandırma çözümlerinde dikkate alınmaz ve bunlar için herhangi bir bastırma veya eleme önlemi alınmaz. Sahteciliğin bastırılması ise, alınan sinyaldeki sahtecilik sinyalinin tespiti temelinde sahteciliğin bastırılması veya ortadan kaldırılması anlamına gelir. Böylece sahtecilik sinyali, gerçek uydu sinyalinin normal konumlandırma ve çözme sürecini etkilemez.

Bilimsel çalışmalarda, sahtekarlık saldırılarına karşı başlıca iki tür yöntem bulunmaktadır. Birinci tür, ek donanım tesislerinin eklenmesini gerektirir. Bu tesisler arasında temelli anten dizileri, temelli çoklu korelatör, sinyal varış açısına dayalı müdahale yöntemleri vb. bulunur. Diğer tür ise sahtecilik algılama veya bastırma yöntemleridir. Bu yöntemler, sinyal parametreleri gibi faktörlere dayanarak sahtecilik sinyalini tanımlamayı ve keşfetmeyi amaçlar.

Sahteciliği önleme tekniklerini, ek donanım kullanıp kullanmamaya göre kategorize ediyoruz. Ek donanım olanaklarından bağımsız sahteciliği önleme yöntemleri, Doppler kayması tabanlı, tutarlılık kontrolü tabanlı, sinyal parametre istatistik analizi tabanlı, varış zamanı ve varış zamanı farkı tabanlı ve artık sinyal tespiti tabanlı alt kategorilere ayrılmıştır.

Tablo 3.5 Aldatma Tespit Yöntemlerinin Sınıflandırılması Bölüm 1

Yöntem	**Açıklama**
Doppler Kayması [29], [30], [31], [32], [33], [34]	Yüksek hızda seyreden bir navigasyon uydusu ile hedef alıcı arasındaki göreceli hareketten kaynaklanan Doppler kaymasını kullanarak sahteciliği tespit eder.
Tutarlılık Kontrolü [35], [36], [37]	Sahte ve gerçek sinyaller arasındaki tutarsızlıkları izleyerek, sahteciliği tespit etmek için sinyal parametrelerini dikkatle inceleyen bir yöntemdir. Örneğin, genliği, taşıyıcı-gürültü oranı, faz ve diğer parametrelerdeki anormal değişiklikleri izleyebilir.
Sinyal Parametre İstatistik Analizi [38], [39], [40], [41], [42], [43], [44]	Sinyal parametrelerinin istatistiksel analizini kullanaraksahteciliği tespit eder. Bu yöntem, istatistik teorisinde verileri test etmek için kullanılan değişken analizi yöntemini GNSS sahteciliği tespiti alanına uygular. Sinyal parametrelerinin taklit edilmesinin zor olduğu özelliklerine dayanır ve istatistiksel testlerle sahtecilik sinyallerini tanımlamak için karar eşiği ve karar istatistiği belirler.
Varış Zamanı ve Varış Zamanı Farkı [45], [46]	Sahte ve gerçek uydu sinyallerinin varış zamanlarındaki farklılıkları izleyerek sahteciliği tespit eder. Örneğin, uydu sinyallerinin gerçekten geldiği kaynaktan alıcıya ulaşması için gerekli olan mesafe ve süre ile sahte sinyallerin ulaşması için gereken mesafe ve süre arasındaki farkları kullanabilir.

Ek donanım olanakları kullanan sahteciliği önleme yöntemleri ise anten dizisi tabanlı, varış açısı tabanlı, alt uzay projeksiyonu tabanlı, sinyal varış yönü tabanlı ve sinyal kalitesi izleme tabanlı olarak alt kategorilere ayrılmıştır.

Tablo 3.6 Aldatma Tespit Yöntemlerinin Sınıflandırılması Bölüm 2

Yöntem	Açıklama
Artık Sinyal [47], [48]	Alıcı sahtecilik sinyalini aldığında, gerçek uydu sinyalini tamamen ortadan kaldırmak zordur. Bu yöntem, gerçek uydu sinyalini tespit ederek sahteciliği ortadan kaldırır. Örneğin, alınan sinyaldeki sahtecilik sinyali için artık sinyal algılama işlemini tamamlamak için gerçek uydu sinyal bileşenini kullanabilir.
Anten Dizisi [49], [50], [51], [52]	Anten dizilerine dayalı sahtecilik tespit yöntemi, uzamsal filtreleme tekniklerini kullanır. Bu yöntem, belirli bir açı için bir kazanç sağlar ve belirli bir uzamsal sektörü zayıflatır. Statik ve dinamik sahtekarlık senaryolarında pratik ve etkili bir sahtekarlık önleme yöntemidir.
Varış Açısı [41], [48]	Sahte ve gerçek uydu sinyallerinin geliş açıları arasındaki farklılıkları izleyerek sahteciliği tespit eder. Bu yöntem, sahte ve gerçek sinyallerin alıcı antenin faz merkezine ulaşan yön açılarını izler ve sahtecilik sinyallerinin daha tutarlı bir şekilde geldiğini gözlemleyebilir.
Alt Uzay Projeksiyonu [49], [53]	Alt uzay projeksiyonu, zaman-frekans alanını analiz etmek için kullanılan bir sinyal işleme yöntemidir. Altuzay oluşturmak için gereken uygun bilginin seçilmesi, altuzay projeksiyon teknolojisinin önemli bir parçasıdır. Uzaysal alan sahtekarlık sinyalinin alt uzay projeksiyonu çözülerek, gerçek uydu sinyalinden daha büyük güce sahip sahtekarlık sinyali ortadan kaldırılabilir.
Sinyal Geliş Yönü [4], [54]	Elektromanyetik dalganın geliş yönünü izleyerek sahteciliği tespit eder. Bu yöntem, sahte ve gerçek sinyaller arasında uzamsal korelasyon olduğu gerçeğine dayanır. Örneğin, aynı sahtekarlık sinyali vericisi tarafından iletilen farklı uydu sinyalleri genellikle aynı yönden gelirken, gerçek uydu sinyalleri farklı yönlerden gelir.
Sinyal Kalitesi İzleme [25], [55], [56], [57], [58]	Sahte ve gerçek sinyallerin varış zamanlarındaki farklılıkları izleyerek sahteciliği tespit eder. Örneğin, alıcıda çoklu korelatör ile konfigüre edilmişse, sahtekarlık sinyalinin varış zamanı ile gerçek uydu sinyalinin varış zamanı arasındaki farklar, korelasyon zirvesinde bir anormalliğe neden olabilir ve bu durum sahteciliği tespit etmek için kullanılabilir.

3.3.1 Doppler Kaymasına Dayalı Tespit Yöntemi

Yüksek hızda seyreden bir navigasyon uydusu ile hedef alıcı arasındaki göreceli hareket, Doppler kaymasını tetiklemektedir. Alıcı izleme birimi, tüm uydu sinyallerini dikkatle izlemekte ve bu sinyallerin genliği, taşıyıcı-gürültü oranı, faz ve Doppler kayması gibi çeşitli parametrelerini sahtecilik tespit birimine sunmaktadır. Eğer hedef alıcı tarafından gerçekte alınan uydu sinyalinin Doppler kayması değerinde önceden belirlenmiş bir eşik değerini aşan ani bir değişiklik tespit edilirse, bu durum GNSS alıcısının sahtecilik saldırısı gibi bir güvenlik tehdidiyle karşı karşıya olduğunu göstermektedir. Dolayısıyla, Doppler kayması değişimini izlemek, sahtekarlık sinyallerine karşı etkili bir savunma stratejisi sunmaktadır. Doppler kaymasına dayalı aldatma tespit senaryosu Şekil 3.3'te gösterilmiştir.

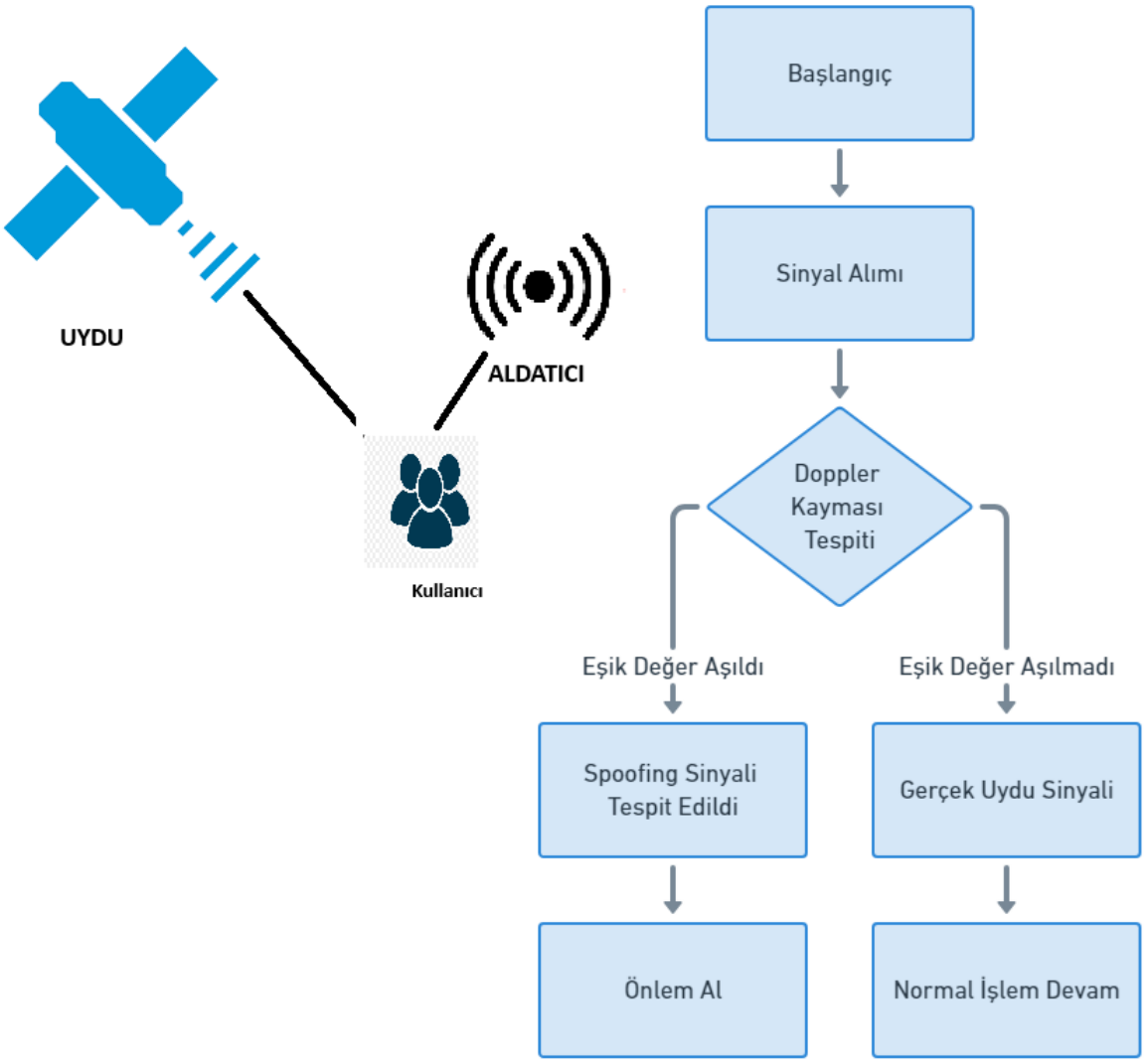
Uydu sinyallerinin yakalanması, işlem sürecinin temel ve kritik bir aşamasıdır. Eğer sinyal yakalama aşamasında sahtecilik başarılı bir şekilde tespit edilip bastırılabilirse, alıcı mümkün olan en kısa sürede uyarılarak yanlış navigasyon ve konumlandırma çözümlerinin kullanılmasının önüne geçilebilir.

3.3.2 Tutarlılık Kontrolüne Dayalı Tespit Yöntemi

Sahte sinyal ve gerçek uydu sinyali için bileşik sinyalin sinyal parametreleri normal makul aralığın ötesine geçebilir veya bu aralığı atlayabilir. Bu sinyal parametrelerindeki anormal değişiklikler ve sahtecilik sahnesi ile normal iletim ortamı arasındaki farklar göz önüne alınarak, sahtecilik sinyalinin etkili bir şekilde algılanması sağlanabilir.

3.3.3 Sinyal Parametre İstatistik Analizine Dayalı Tespit Yöntemi

İstatistik teorisinde verileri test etmek için kullanılan değişken analizi yöntemi GNSS sahteciliği tespiti alanına uygulanabilir. Sinyal parametre istatistiklerinin taklit edilmesinin zor olduğu özelliklerine dayanan şema, örnek ortalama değer testi, karesel toplam, varyans, maksimum olabilirlik tahmin testi gibi istatistiksel yöntemleri kullanır ve faz uzayı özelliği



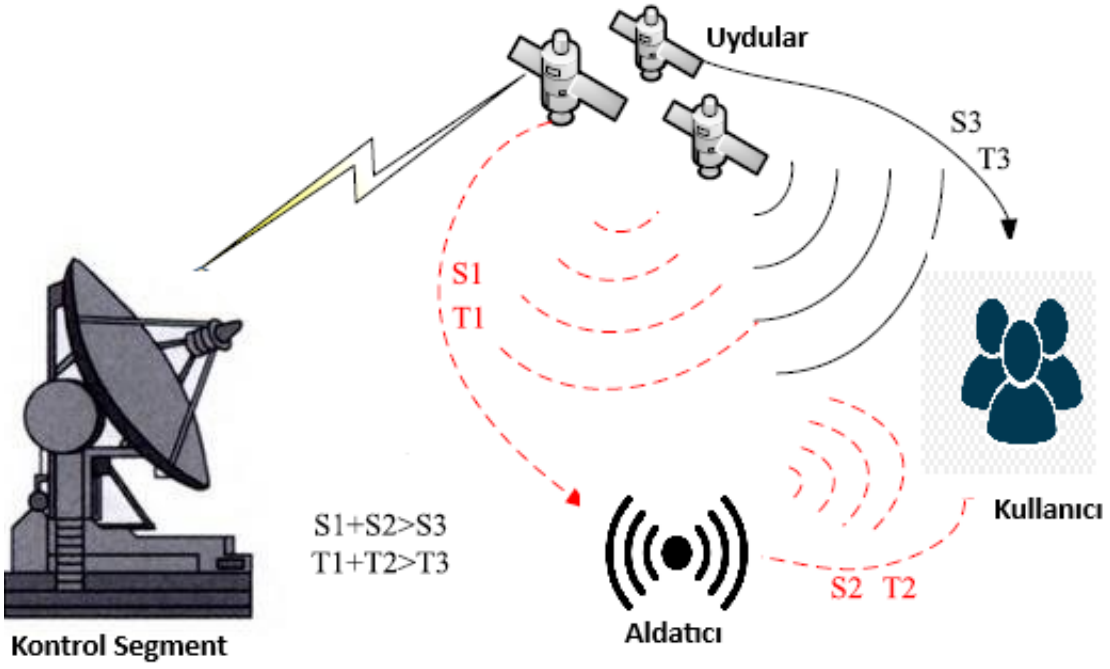
Şekil 3.3 Doppler Kaymasına Dayalı Tespit

ve taşıyıcı faz ölçümleri gibi parametreleri birleştirerek sahteciliğin etkili tanıma sürecini tamamlamak için karar eşiği ve karar istatistiği belirleme gibi yöntemleri benimser.

3.3.4 Varış Zamanı ve Varış Zamanı Farkına Dayalı Tespit Yöntemi

Şekil 3.4'te gösterildiği gibi, uydu sinyallerini yayınlayan gerçek uydudan ileri tip sahtekarlık kaynağına sinyal iletim mesafesi (S1) ve süresi (T1) ile ileri tip sahtekarlık kaynağından hedef alıcıya sinyal iletim mesafesi (S2) ve süresi (T2) kaçınılmaz olarak gerçek uydudan hedef alıcıya doğrudan iletilen uydu sinyalinin iletim mesafesinden (S3) ve iletim

süresinden (T3) daha uzundur. Bunun nedeni, ileri yönlü sahtekarlık sinyalinin alıcıya ulaşan daha uzun bir yolu iletmek için belirli bir gecikme süresini geçmesi gerektiğidir. Alıcıların hedef anteninin faz merkezine ulaşan uydu sinyalleri arasındaki zaman farkı makul aralığın dışındaysa, alıcı sinyalinin sahtekarlık sinyali ve gerçek uydu sinyalinden oluşan bir bileşik sinyal olması muhtemeldir. Şu anda, sahtekarlık tespit yöntemleri üzerine birçok araştırma vardır ve sahtekarlık tespiti kadar önemli olan sahtekarlık konumu üzerine çok az araştırma vardır. Aslında, sahteciliğin kaynağını bulmak çok gereklidir, çünkü sahteciliğin kaynağını doğru bir şekilde bulmak, aldatıcıyı tanımlamak ve ortadan kaldırmak için faydalıdır.



Şekil 3.4 Varış Zamanı ve Varış Zamanı Farkına Dayalı Tespit

3.3.5 Artık Sinyale Dayalı Tespit Yöntemi

Alıcı sahtecilik sinyalini aldığında, gerçek uydu sinyalini tamamen ortadan kaldırmak zordur. Sahtecilik saldırısının gerçek uydu navigasyon sinyalini etkili bir şekilde bastıramayacağı varsayımı altında, alınan sinyaldeki sahtecilik sinyali için artık sinyal algılama işlemini tamamlamak için artık gerçek sinyal bileşeni kullanılabilir. Artık sinyal tespiti, ilk başlangıçta mevcut alınan sinyalde belirli bir uydunun sahtekarlık sinyalinin olup olmadığını

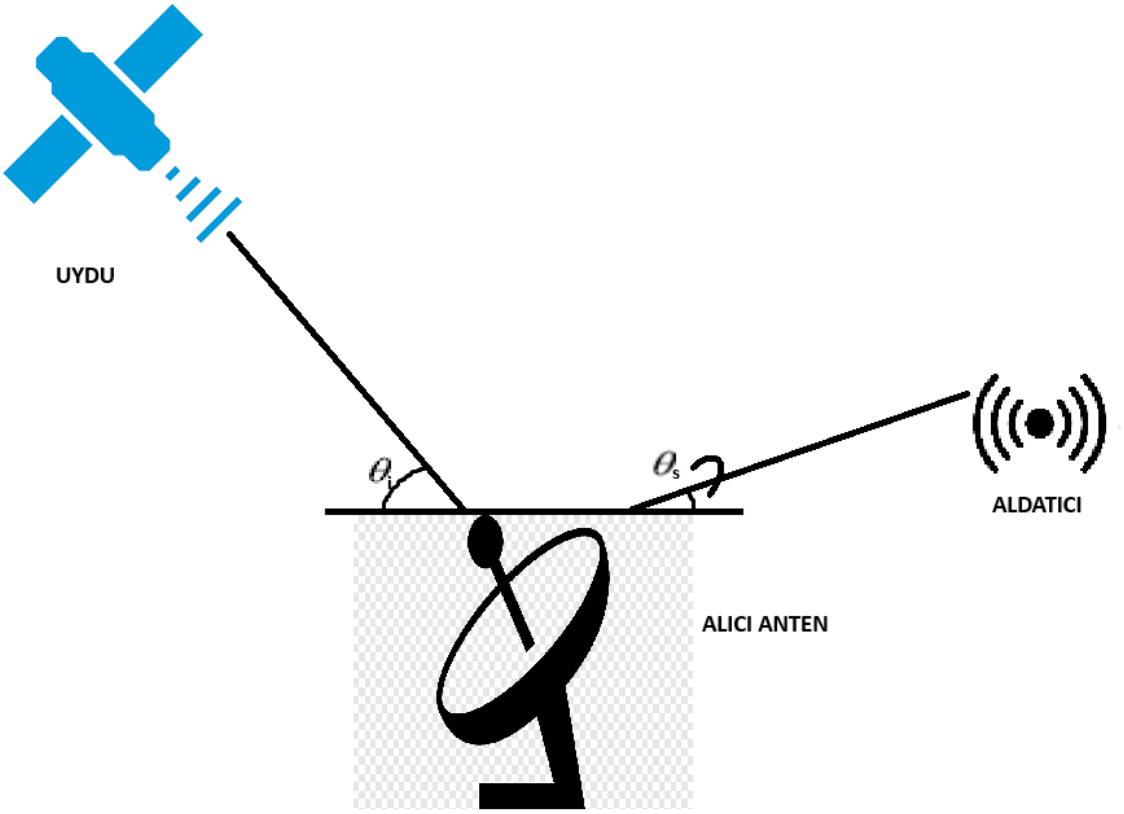
tespit etmek için alıcı edinme aşamasında gerçekleştirilir. Takip aşamasındaki artık sinyal tespiti ise gerçek uydu sinyalini takip eden alıcıda mevcut olabilecek sahteciliği gerçek zamanlı olarak tespit etmek içindir.

3.3.6 Anten Dizisine Dayalı Tespit Yöntemi

Anten dizilerine dayalı sahtecilik tespit yöntemi, alınan bir sinyal demetini oluşturmak için uzamsal filtreleme tekniklerini kullanır. Bu yöntem belirli bir açı için bir kazanç sağlar ve belirli bir uzamsal sektörü zayıflatır. Statik ve dinamik sahtekarlık senaryolarında pratik ve etkili bir sahtekarlık önleme yöntemidir. Yöntem, anten dizisine gelen sahtecilik sinyallerinin hepsinin aynı yönden geldiği, ancak anten dizisine gelen gerçek uydu sinyallerinin farklı yönlerden uzamsal özelliklere sahip olduğu varsayımına dayanır. Bu yöntemin uygulanması genellikle ek donanım gerektirir ve hatta anten dizisinin düzeltilmesini ve yakalama ve izleme aşamalarında alıcı mimarisinde bir dereceye kadar değişiklik yapılmasını gerektirir.

3.3.7 Varış Açısına Dayalı Tespit Yöntemi

Şekil 3.5'te gösterildiği gibi, gerçek uydu navigasyon sinyalinin alıcı antenin faz merkezine ulaşan yön açısı (θ_i) tamamen tutarlı değildir ve aynı verici tarafından iletilen sahtecilik sinyalinin alıcı antenin faz merkezine ulaşan yön açısı (θ_s) tamamen tutarlıdır. Bu nedenle yöntem, sahtecilik sinyalinin tanımlama özelliği olarak sahtecilik sinyali ile gerçek uydu sinyali arasındaki önemli varış açısı farkına dayanır ve sahteciliği tespit etmek için uydu sinyalinin uzamsal özelliklerini kullanır. Genel olarak, her ek sahtekarlık vericisi, ona karşılık vermek için ek bir anten gerektirir. Anten sayısının artırılması, bir sahtekarlık saldırısının başarılı bir şekilde uygulanması için teknik zorluğu artırabilir. Bu nedenle, anten sayısı uygun şekilde artırılabilirse, sahteciliği önleme algılama performansı bir dereceye kadar iyileştirilebilir.



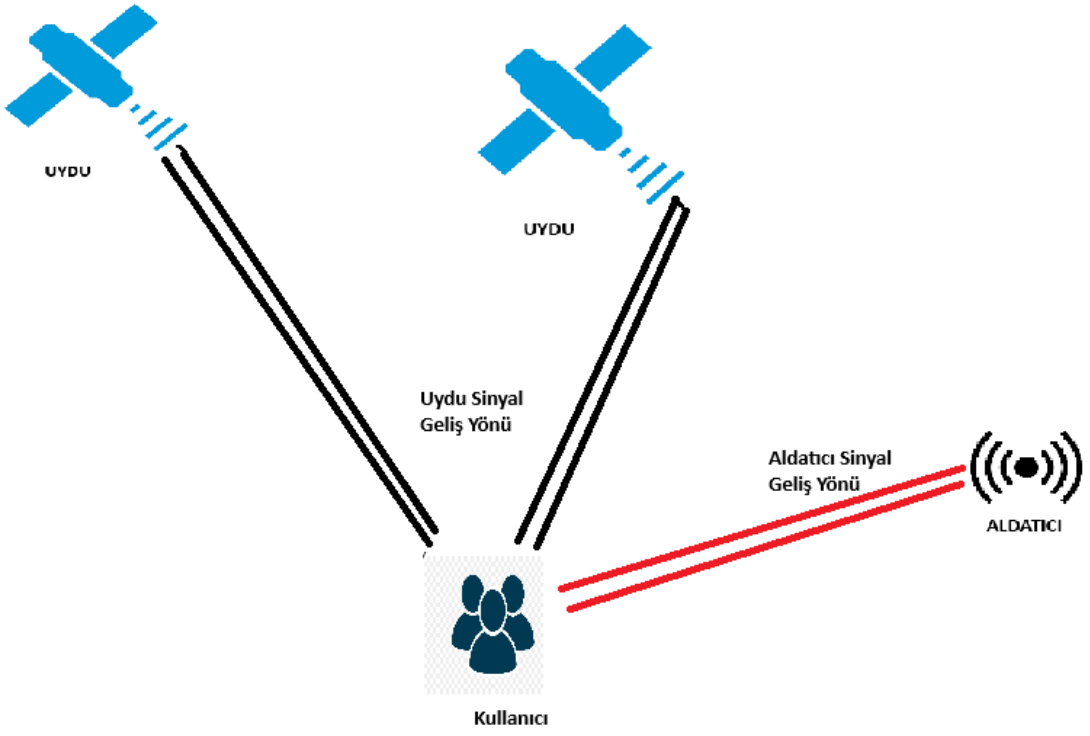
Şekil 3.5 Varış Açısına Dayalı Tespit

3.3.8 Alt Uzay Projeksiyonuna Dayalı Tespit Yöntemi

Alt uzay projeksiyonu yaygın olarak kullanılan bir sinyal işleme yöntemidir. Altuzay oluşturmak için gereken uygun bilginin seçilmesi, altuzay projeksiyon teknolojisinin önemli bir parçasıdır. Uzaysal alan sahtekarlık sinyalinin alt uzay projeksiyonu çözülerek, gerçek uydu sinyalinden daha büyük güce sahip sahtekarlık sinyali ortadan kaldırılır. Alt uzay projeksiyon tekniği zaman-frekans alanını analiz etmek için kullanılır. Girişim alt uzayı tahmin yöntemi, girişim alt uzayını oluşturmak ve giriş sinyali verilerini girişim alt uzayına ortogonal alt uzaya yansıtmak için kullanılır. Yaygın olarak kullanılan bir sahtekarlık önleme yöntemidir.

3.3.9 Sinyal Geliş Yönüne Dayalı Tespit Yöntemi

Şu anda taklit edilmesi zor olan tek sinyal özelliği elektromanyetik dalganın yönüdür. Şekil 3.6'da gösterildiği gibi, bir sahtecilik sinyali kaynağı tarafından yayılan sinyaller arasında uzamsal korelasyon vardır. Mevcut teknik koşullar nedeniyle, birkaç farklı uydunun sahtecilik sinyalleri genellikle aynı sahtecilik sinyali vericisi tarafından iletilir ve gerçek uydu sinyalleri sahtecilik sinyallerinin uzamsal korelasyonuna sahip değildir, bu nedenle sahtecilik tespiti bu gerçeğe dayanabilir.



Şekil 3.6 Sinyal Geliş Yönüne Dayalı Tespit

3.3.10 Sinyal Kalitesi İzlemeye Dayalı Tespit Yöntemi

İletilen sahtecilik sinyalinin alıcıya ulaştığı zaman ile gerçek sinyalin alıcıya ulaştığı zaman arasında belirli bir gecikme vardır. Çoklu korelatör ile konfigüre edilmiş alıcı için, sahtekarlık sinyalinin varış zamanı ile alıcıya gelen gerçek uydu sinyali arasındaki fark, korelasyon

zirvesinde bir anormalliğe neden olur. Sahte sinyal alıcı korelatör çıkışını etkiler. Bu nedenle, korelasyon tepe noktasındaki bozulma ile sahtecilik sinyali olup olmadığına karar vermek mümkündür.

3.3.11 Diğer Tespit Yöntemleri

Yukarıda açıklanan sahteciliği önleme yöntemleri, sahteciliği tespit etme veya sahteciliği bastırma seviyesinden sahteciliğe karşı direnç uygular. Yukarıdaki yöntemler teknik detaylar açısından on kategoriye ayrılmıştır. Aldatma karşıtı yöntemlerin bazı uygulama araçları ve teknik detayları yukarıdaki on kategori ile tutarlı değildir. Farklı donanımlarla faz açısı gibi parametrelerin ölçümlerinin yapıldığı, yapay zekanın kullanıldığı karşı tedbir yöntemleri vardır. [59], [60], [61–65]

3.4 Literatürde Karşı Tedbir Tekniklerinin İncelenmesi

Yuan'ın çalışmasında [29], sahteciliği tespit etme ve azaltma özelliğine sahip yeni bir GNSS toplama yöntemi önerilmektedir. Bu yöntem, sadece GNSS sinyallerini almakla kalmaz, aynı zamanda kod ve taşıyıcı Doppler'lerin ortak tutarlılık tespitine dayanarak sahtecilik sinyallerini tespit edebilir ve azaltabilir. Performans analizi ve sayısal simülasyon sonuçları, önerilen yöntemin bir veya daha fazla sahtecilik sinyali olduğunda geçerli olduğunu göstermektedir. Yöntem, öncelikle Hough Dönüşümü kullanılarak gerçek ve sahte sinyallerin kod ve taşıyıcı Doppler'lerini hesaplar. Ardından, alınan sinyaller, kod ve taşıyıcı Doppler'lerin ortak tutarlılık tespitine dayalı olarak gerçek ve sahte sinyaller olarak sınıflandırılır. Son olarak, otantik sinyalin parametreleri alıcının izleme döngüsüne aktarılır. Bu yöntemin bazı avantajları bulunmaktadır. İlk olarak, sinyal toplama ve sahteciliği azaltma işlemlerini aynı anda gerçekleştirebilir. İkinci olarak, zamanında ve ardışık sahtecilik azaltma gerçekleştirilebilir. Üçüncü olarak, mevcut alıcı toplama modülünde sadece küçük bir değişiklikle düşük maliyetle uygulanabilir. Önerilen yöntem, sadece gerçek ve sahte sinyalleri tespit etmekle kalmaz, aynı zamanda tanımlayabilir ve sahtecilik azaltma için etkili olduğunu gösterir.

Doppler ile ilgili bir diğer çalışma da Jovanovic ve arkadaşlarının [30], sırasıyla sinyal gücü değişimini ve taşıyıcı Doppler kaymasını tespit etmek için Güç Eşiği Dedektörü (Power Threshold Detector, PTD) ve Doppler Ofset Dedektörü (Doppler Offset Detector, DOD) kullanarak uyarlanabilir izleme algoritması kavramını önermesidir. [31]'da ise araç ağlarındaki Doppler kayması temelli bir GNSS karşı-sahtecilik teknolojisi önerilmektedir. Tek bir sahtecilik kaynağının bulunduğu durumda, bu makalede sunulan iki yöntemle düşük maliyetle sahtecilik tespiti gerçekleştirilebilir. Teknoloji oldukça etkilidir ve simülasyon sonuçlarıyla doğrulanmıştır. Broumandan ve arkadaşlarına göre [32] aynı vericiden gelen farklı GNSS sinyallerinin temelde aynı uzamsal imzası olduğu için, sahtecilik sinyallerini ayırt etmek için kullanılabilir. Otomatik olarak yön değiştiren bir anten kullanılarak, görünür uydu sinyallerinin genlik ve Doppler korelasyonunu izleyerek, gerçek ve sahte sinyallerin uzamsal imzaları arasındaki farkı ayırt etmek için incelenmiştir. Bu tespit yönteminin etkinliği bir dizi deney temelinde incelenmiş ve doğrulanmıştır. Van ve arkadaşları çalışmalarında [33], GPS sinyallerinde Doppler etkisini kullanarak sinyal bütünlüğünü izlemeyi ve sahtecilik girişimlerini tespit etmeyi araştırmıştır. Alıcı, taşıyıcı frekansın Doppler kaymasını kesin olarak belirleyerek kendi hareketini hesaplayabilir. Hesaplanan hız ve rotanın geleneksel olarak elde edilenlerle karşılaştırılması, gerçek ve sahte sinyaller arasındaki ayrımı sağlar. Sonuçlar, önerilen yöntemin GPS sinyallerinin Doppler kaymasını doğru bir şekilde tahmin ettiğini göstermektedir, bu da sahtecilik tespitini 1 Hz'lik bir doğrulukla mümkün kılar. Bu yaklaşım, GPS tabanlı sistemlerin bütünlüğünü ve güvenliğini korumak için hayati öneme sahip olan GPS sahteciliğini tespit etmek için güvenilir bir yöntem sağlar. [34]'e göre sahtecilik sinyalinin taşıyıcı Doppler'i, orijinal sinyalininkine kilitlemediğinde, bu tür bir sahtecilik sinyalinin spektrumunda çift tepe oluşur. Girişimsiz bir durumda, çift tepe olmamalıdır. Çoklu yol senaryosunda, çift tepe mevcut olabilir, ancak çift tepe sinyallerinin sayısı ve çift tepe sinyallerinin göreceli hız artığı miktarları, sahtecilik senaryosundaki gibi farklıdır. Bu çalışmada, frekans alanındaki çift tepe ve göreceli hız artığına dayalı bir ara katman sahtecilik tespit tekniği önerilmektedir. Bu yöntem, sahteciliği tespit etmenin yanı sıra sahtecilik senaryosunu çoklu yol senaryosundan ayırabilir. Hızlı Fourier dönüşümü tabanlı yöntemler, çift tepeyi tespit etmek ve çift tepe Doppler farkını çıkarmak için kullanılır, ve Doppler farkına dayalı göreceli hız

artığı hesaplaması türetilir. Bu yaklaşımın performansı hem analitik hem de deneysel olarak değerlendirilmiştir: simülasyon sonuçları, çoklu yol senaryosundaki sahtecilik yanlış alarm olasılığının düşük olduğunu göstermektedir, bu da sahtecilik senaryosunun ve çoklu yol senaryosunun iyi bir şekilde ayırt edilebileceğini göstermektedir; ve etkinlik, Texas Sahtecilik Test Pilinde (TEXBAT) temellendirilmiştir.

Tutarlılık kontrolüne dayanan çalışmalar için [35]'te önerilen yöntem, sinyali doğrulamak için alıcı mobil antenini kullanır ve alıcı izleme aşaması sırasında alıcı mobil anteninin kanal yanıtına göre karşılık gelen genlik, faz ve Doppler değişikliklerinin yüksek korelasyonunu tespit eder. Konumlandırma navigasyon aşamasında, sahtekarlık sinyali mobil alıcı seviyesi için gözlemlenebilir bir konumda tespit edilebilir. IMU'nun GNSS ölçümleri ile birleştirilmesi ve kullanıcı hareket modunun sahtecilik için algılama ve sınıflandırma problemine entegre edilmesi, sahteciliğin algılama performansını artırabilir. Ağ tabanlı veya bulut tabanlı uydu sinyali doğruluğu doğrulama yöntemi, alıcılar arasında daha düşük hızlı bir iletişim bağlantısı olduğunu veya iletilen ölçüm verilerinin bulut tarafından depolanabileceğini varsayar [37].

Yurtiçinde ve yurtdışında birçok akademisyen, istatistiksel analize dayalı bir aldatma tespit yöntemi önermiştir. Borio, 2013 yılında bilinen ortalama genlik ve bilinmeyen ortalama genlik varsayımı altında yeni bir faz varyans analizi (PANOVA) test yöntemi önermiştir [38]. Örnek ortalama değerindeki farkı tespit ederek, aldatma saldırıları için etkili tespit elde etmek için uydu sinyalinin faz uzamsal özellikleri belirlenir. Borio ve Gioia bu araştırma alanında devam araştırmaları yürütmüştür. 2016 yılında, Kareler Toplamı (Sum of Square, SoS) tabanlı varış açısı sahteciliği tespit yöntemi önerilmiştir. Kareler toplamı dedektörünü gerçekleştirmek için genelleştirilmiş olabilirlik oranı testi (GLRT) yöntemi kullanılmıştır. SoS karar istatistiği, uzamsal olarak ayrılmış iki GNSS alıcısının taşıyıcı faz ölçümleri kullanılarak hesaplanır. Sözde koda ve onun tamsayı kısmına bir düzeltme olarak ifade edilebilen bir taşıyıcı faz tek fark karesel toplam dedektörü tasarlanmıştır. Bu yöntem karar eşiği kriterini basitleştirir ve sahtekarlık konumu veya anten kalibrasyon işlemi gerektirmez. Yüksek gerçek zaman gereksinimi olan durumlara uygulanabilir [39]. Falletti ve arkadaşları, post-korelasyona dayalı pratik bir sahtecilik tespit yöntemi önermiş

ve bir dizi statik ve dinamik saha deneyi ile sahtecilik sinyallerini tespit etmede etkinliğini kanıtlamıştır [40]. Navigasyon ve konumlandırma çözümünde, sahtecilik saldırılarına maruz kalan navigasyon uyduları, sahtecilik uydu sinyallerinin navigasyon sonuçları üzerindeki yanıltıcı etkisini ortadan kaldırmak ve azaltmak için bir strateji benimser. Hwang ve arkadaşları, alıcının saat kararlılığını kısa sürede analiz etmek için alıcının tahmini saat durumu Allan varyansını kullanan ve sahtecilik kaynağı ile GNSS alıcısı arasındaki göreceli hareketten kaynaklanan dinamik bir sahtecilik olup olmadığını belirleyen bir alıcı otonom sinyal kimlik doğrulama yöntemi önermiştir [41]. Tsinghua Üniversitesi'nden Yuan ve arkadaşları, dizi olasılık oranı testine dayalı GNSS sahteciliği tespit yönteminin gerekli gözlem sayısını önceden belirlemesine gerek olmadığını öne sürmüştür [42]. Önceden belirlenmiş gözlem sayısına dayalı güvenilir tespit yöntemiyle karşılaştırıldığında, gerekli gözlem sayısı büyük ölçüde azaltılabilir. Farklı navigasyon uyduları arasındaki tutarlılığı kullanan Maksimum Olabilirlik Tahmini (MLE), alıcı doğrudan konum tahmininde yaygın olarak kullanılmaktadır ve sahtekarlık saldırılarını bastırmak için kullanılabilir. Wang ve arkadaşları optimum MLE çözümünü bulma problemini çözmüş ve temel parçacık sürüsü optimizasyon algoritmasının erken yakınsama problemini çekici ve itici parçacık sürüsü optimizasyonu (ARPSO) kullanarak çözmüştür [43]. Gross ve arkadaşları, PD dedektörü tabanlı simetrik diferansiyel bozulma ölçüm yöntemi yerine tek sinyal korelasyon fonksiyonu modeline dayalı maksimum olabilirlik tahmini kalıntısını uydurma yöntemini kullanarak bu sorun üzerinde daha derinlemesine bir çalışma yürütmüştür [44]. Geliştirilen teknoloji PD-ML dedektörü olarak adlandırılır ve çok yollu parazit ortamlarında sahtekarlık tanıma performansını önemli ölçüde artırır.

Sahtekarlığın yerini belirleme yöntemi temel olarak varış zaman farkı tahminine dayanır ve varış zaman farkı genellikle sinyal çapraz korelasyon ilişkisine göre ölçülür. Zhang ve arkadaşları diferansiyel kod fazına (DCP) dayalı bir sahtekarlık TDOA tahmin yöntemi önermiş ve DCP tabanlı bir TDOA modeli ve tahmin hata modeli oluşturmuştur [45]. Bu yöntem mevcut yöntemlere göre daha yüksek hassasiyete ve daha iyi performansa sahiptir. Ara sahteciliğin güç seviyesi gerçek sinyalin güç seviyesinden sadece biraz daha yüksek olduğundan, güç tespitine dayalı sahtecilik önleme yöntemi başarısız olur ve diğer

mevcut sahtecilik önleme yöntemlerini kullanarak gerçek zamanlı ara sahtecilik tespiti yapmak zordur. Bu soruna yanıt olarak Li ve arkadaşları, herhangi bir sinyal aralığında eşik korelasyon tepe noktalarının sayısını aşan çok modlu bir algılama yöntemi kullanarak, uydu sinyal toplama modülü tarafından elde edilen izleme sinyalinin tepe değerini toplama işlemi sırasında belirleyebilir [66]. Şema, sahtekarlık sinyali olup olmadığını belirlemek için eşik korelasyon tepe sayısını aşan çok modlu bir algılama yöntemi kullanır ve bir değerlendirme kriteri tanımı, bir performans değerlendirme yöntemi ve ampirik bir formül verir.

Ali al. ortak sinyal kalitesi izleme teknikleri ve artık sinyal izleme kullanan bir sahtecilik tespit algoritması önermiştir [47]. Çok yollu girişim ve sahteciliğin neden olduğu korelasyon fonksiyonu bozulması, oran metriğine ve 3 çift ek korelatöre dayalı iki gösterge ile ayırt edilir ve korelasyon fonksiyonu kalitesi artık sinyali tespit etmek için değerlendirilir. Wei ve diğerleri, sıkıca bağlanmış MEMS INS/GNSS entegre navigasyon sistemi için sahtekarlık profili tahminine dayalı bir GNSS sahtekarlığı tanımlama yöntemi önermiştir. Bu yöntem, sahtekarlık saldırıları nedeniyle genişletilmiş Kalman filtresinin artık bozulma özelliklerini kullanır, sahtekarlık profilini tersine yeniden yapılandırır ve sahtekarlığı tanımlar [48].

Felski, anten ışını sektörü tarafından kapsanan bağımsız alıcı cihazın navigasyon parametrelerini belirlemesini ve navigasyon ve konumlandırma çözümündeki diğer navigasyon izleme cihazlarının parametre bilgileriyle tutarsız olan bilgileri göz ardı etmesini önermiştir [49]. Yöntem, özel dijital donanım ve yazılım kontrollü çok elemanlı anten dizileri gibi bazı yerleşik mekanizmalar ekleyerek sahte sinyallerin etkilerini ortadan kaldırır. Huet ve arkadaşları dizi tabanlı kör adaptif dizi sinyal işleme yöntemi önermişlerdir [50]. Bu yöntem sadece periyodik olmayan parazit, periyodik parazit ve sahtekarlık saldırısı DOA'sında uyarlanabilir bir şekilde derin boşluklar oluşturmakla kalmaz, aynı zamanda bant içi sahtekarlığı azaltabilir ve yararlı sinyalleri geliştirebilir. Jiang ve arkadaşları, tek sabit taban çizgisi, sabit ve bağımsız taban çizgisi ve çift bağımsız taban çizgisi Max/Min modeli için üç durumu göz önünde bulundurarak, taban çizgisi verilerinin istatistiksel analizine dayalı sahteciliği tespit etmek için bir yöntem önermiş ve taban çizgisi değerlerinin algılama performansı üzerindeki etkisini analiz etmiştir [51]. Çift anten senkronize değilse, diğer sahtekarlık tespit yöntemlerinin başarısız olması muhtemeldir, ancak diferansiyel güç

oranı sahtekarlık tespiti için hala kullanılabilir. Wang ve arkadaşları tarafından önerilen sözde menzil ve taşıyıcı faz ölçümü asenkron modelleri ve çift anten güç ölçümüne dayalı sahtecilik tespit yöntemi, senkronize olmayan durumlarda sahteciliği tespit edebilir [52]. Yukarıdaki çeşitli sahtecilik tespit yöntemleri, alıcı tarafından yakalama veya izleme sürecinde sahtecilik sinyallerinin tanımlanmasını ve keşfedilmesini gerçekleştirmek içindir. Aşağıdaki iki yöntem, alıcının despreading aşamasında tamamlanan sahtekarlık tespit sürecidir. Sahte sinyalin aynı sahte kaynaktan geldiği varsayımı altında, Daneshmand ve arkadaşları sahte sinyalin yönlendirme vektörünü çıkaran ve alıcı yayılmadan önce sahte sinyali atan bir sahtekarlık bastırma yöntemi önermiştir [55]. Sahtecilik tespit ve bastırma sürecinin tamamında, dizi işleme ön yayılım aşamasında gerçekleştirilir ve tüm sahtecilik sinyallerinin ve gerçek sinyallerin sözde rasgele kodunu izlemeye gerek yoktur. Yaklaşım, sahtekarlık korelasyon zirvesini ortadan kaldırmak ve sahtekarlığın neden olduğu gürültü seviyesini zayıflatmak için sahtekarlık sinyalindeki uzamsal özellikleri çıkarır. Aynı zamanda yöntem, tek bir gerçek sinyalin sinyal-gürültü oranını en üst düzeye çıkarmak için anten çıkış kısmını genişletir. Kör ön-ayrıştırma tekniği etkili ve düşük karmaşıklıkta bir sahtecilik bastırma yöntemidir. [35]'de önerilen sahtekarlık tespit yöntemi, ön yayma aşamasında dizi kalibrasyonu yapmaya ve alıcı yapısını değiştirmeye gerek duymaz, bu da hesaplama karmaşıklığını azaltır. Yayma sonrası aşamada ise şemanın iki durumda dikkate alınması gerekir. Bu yöntem, düşük güçlü ve yüksek güçlü sahtekarlık saldırılarını etkili bir şekilde tespit edebilir [35].

Han ve arkadaşları, sahtekarlık sinyalinin sinyal gücünün gerçek sinyal gücünden daha büyük olduğu varsayımı altında, alınan navigasyon sinyalini sahtekarlık sinyalinin ortogonal sıfır uzayına yansıtmak için sözde rastgele gürültü kodu alanında taşıyıcı frekansı ve kod gecikme parametresi bilgilerinin kullanıldığını bulmuştur [53]. Yukarıdaki süreç sahteciliği tespit edebilir ve ortadan kaldırabilir. Sahtecilik için frekansın hızlı değişimi, alt uzay projeksiyon tekniğine dayanan zaman-frekans alanı sahteciliği önleme yönteminin anlık frekansın yanlışlığına duyarlı olmasına neden olur. Bu soruna yanıt olarak Wang ve arkadaşları, alınan navigasyon sinyalini sahtecilik sinyalinin ortogonal alt uzayına yansıtmak için uyarlanabilir bir projeksiyon modülü kullanmıştır [67]. Yöntem, sahtekarlık algoritmasını uyarlanabilir

blok alt uzay projeksiyon teknolojisi ile optimize ederek korelatör sinyal-gürültü oranının 11 dB artmasını sağlar. Dong ve arkadaşları iki aşamalı bir hibrit girişim bastırma şeması önermiştir [68]. Sahtekarlığın olmadığı durumlarda sigmoid fonksiyonu, gerçek uydu navigasyon sinyalleri üzerindeki etkisini azaltmak amacıyla birinci seviye işlemeyi ayarlamak için kullanılabilir. İkinci aşama, gerçek sinyaller için yüksek ışın kazancı sağlayan anti-parazit ışınları oluşturmak için çapraz spektrumun çapraz skor algoritmasını sunar. Çoğu parazit tespit ve bastırma yöntemi yalnızca tek tip parazit için işlenir. Xu ve arkadaşları, çoklu bilgi kaynaklarına ve parametre tahmin tahminlerine dayalı bir sahtekarlık tespit tekniği önermiştir [54]. İlk aşamada, koordinat kaynağı emisyon kaynağını sınıflandırmak ve yüksek yükseklik açısına sahip bir kaynak seçmek için kullanılır ve yüksek kazanç sağlamak için sensör uzayı yerine ışın uzayı kullanılır. İkinci aşamada, alınan her sinyal eğik projeksiyonla ayrılır, bu da sahtekarlık sinyalini ve çoğu çok yollu sinyali daha iyi tanımlayabilir ve ayırt edebilir.

Manfredini ve arkadaşları sinyal kalitesi izleme teknolojisini (SQMT) kullanan bir sinyal işleme algoritması önermiştir [56]. Yöntem, korelasyon fonksiyonunun tepe kalitesini ölçer ve artık sinyali tespit etmek için bir çift ek korelatör kullanır. Statik ve dinamik koşullar altında ilgili şekillerin ve artık sinyallerin bozulmasını tanımlayabilir ve daha düşük karmaşıklıkla sahteciliği önleme performansını doğrulayabilir. Jahromi ve arkadaşları izleme seviyesindeki sahteciliğin alıcı korelatör çıkışı üzerindeki etkilerini analiz etmiş ve sinyal kalitesi izleme (SQM) metriklerini tasarlamıştır [57]. Yöntem, alıcı izleme aşamasında gerçek bir sinyal korelasyon tepe noktası ile sahte bir sinyal korelasyon tepe noktası arasındaki etkileşimin neden olduğu bir bozulma anomali şeklini veya asimetrik bir korelasyon tepe noktasını tespit eder. Bu yöntem birden fazla sinyal kalitesi izleme (SQM) göstergesinin istatistiksel özelliklerini her bir SQM metriğinin ortalama ve varyansı ile birleştirerek uygun bir sahtecilik tespit eşiği hesaplar. Broumandan ve arkadaşları, sahtekarlık sinyalleri ve çok yollu sinyallerin bir arada bulunduğu çok yollu girişim ortamlarında sahtekarlığı birlikte tespit etmek için yayılma öncesi metrikler ve yayılma sonrası metriklerin kullanılmasını önermiştir [36]. Sinyal kalitesi algılama göstergesi başlangıçta çok yollu girişimden etkilenen korelasyon tepe kalitesini izlemek için kullanılır.

Geliştirilmiş SQM tekniği, izleme aşaması sırasında yayılım sonrası bir metrik olarak sahteciliği tespit edebilir. Yalnızca sinyal kalitesi algılama endeksi ve taşıyıcı-gürültü oranı göstergesi eşiği aşarsa, çok yollu parazitin var olduğunu gösterir; varyans, SPCA, SQM ve taşıyıcı-gürültü oranının tümü eşiği aşarsa, sahteciliğin tespit edildiğini gösterir. [69] makalesinde, GPS aldatma tespiti için kullanılan iki yöntem üzerinde detaylı bir çalışma sunulmuştur, ki bu yöntemler herhangi bir ek donanım gerektirmeden GPS alıcısı içinde uygulanmıştır. İlk olarak, Güç İzleme (Power Monitoring, PM) yöntemi, alıcıya gelen GPS sinyallerinin genliklerini takip ederek kullanılan frekans bandındaki genlik değişimlerini kontrol eder ve aldatma durumunda alıcıya gelen aldatma sinyalinin gerçek GPS sinyalinden daha güçlü olması gerektiğini belirler. İkinci olarak, Tamamlayıcı Sinyal Kalitesi İzleme (Signal Quality Monitoring, SQM) yöntemi, sinyaller arası korelasyona bakarak aldatma tespiti yapar. Novatel G-III alıcısı kullanılarak gerçekleştirilen çalışmada, bu yöntemler simülasyon ortamında ve gerçek verilerle test edilmiş ve başarılı sonuçlar elde edilmiştir. Özellikle, bu teknik, güç ölçümlerinin gözlemi ve korelasyon fonksiyonundaki asimetri kontrolünün birleştirildiği bir yöntem sunmaktadır. Bu çalışma, ticari alıcıların çıktılarını kullanarak sahte sinyal karşıtı tekniklerin etkili bir şekilde uygulanabileceğini göstermektedir.

Borio ve ekibinin çalışmasında [70] tek bileşenli bir GNSS karıştırıcısı tarafından yayılan karıştırma sinyaline karşı geliştirilmiş bir çentik filtresinden bahsedilmektedir. Bu filtre, çoklu durumlu çentik filtresi adını taşır ve hızlı frekans değişimlerini takip etmek için bir frekans tahmini cihazı, karartma sinyalinin alıcı bandı içinde olup olmadığını doğrulayan bir enerji dedektörü ve karartma sinyalinin anlık frekansındaki ani değişikliklerle başa çıkmak için bir sıfırlama dedektöründen oluşmaktadır. Borio ve ekibinin çalışması, bu filtre kullanılarak GNSS alıcısının karıştırma sinyallerinden etkilenmesini engellemenin başarılı bir yolunu ortaya koymaktadır. Li ve ekibinin çalışmasında ise [59], konumlandırma hata düzeltmesi ve M-tahmini teorisi temel alınarak geliştirilmiş bir parçacık filtresi konumlandırma algoritması önerilmektedir. Bu önerilen algoritma, sahte sinyal engellemesini tespit etme ve bastırma adımlarını içermektedir. Sahte sinyal engellemesi tespit edildikten sonra, geliştirilmiş parçacık filtresi algoritması M-tahmini

güçlü istatistik teorisi ile birleştirilerek, yalancı menzil parçacık güncellemesinin ek düzeltme sürecini düzeltmek için kullanılır ve ardından sahte sinyalin etkisini ortadan kaldırır. Li ve ekibinin çalışması, simülasyon sonuçlarıyla önerilen algoritmanın etkinliğini ve üstünlüğünü doğrulamıştır. Bu iki çalışma, çentik filtre tasarımı ve farklı algoritmalar kullanarak GPS sahteciliği ve karartma saldırılarına karşı etkili önlemler geliştirme çabalarını temsil etmektedir.

Yapılan başka bir çalışmada [60] Wei ve ekibi, GPS aldatma saldırılarını tespit etmek için makine öğrenmesi tabanlı bir yöntem geliştirilmiş ve gerçek zamanlı uçuş verileri kullanılarak bu yöntem test edilmiştir. Bu yöntem, ivmeölçer, jiroskop, manyetometre, GPS ve barometre verilerini kullanarak algı verilerine dayanmaktadır. Algılayıcı verilerinin farklı kusurları, seçilen özelliklerin birbirini tamamlamasını sağlayarak kullanılmıştır. Gerçek uçuş verileriyle yapılan deneysel çalışmalar, PERDET'in %99.69 oranında tespit başarısına sahip olduğunu ve mevcut yöntemlerden daha etkili olduğunu göstermektedir. Karşılaştırmalı analizlerde, PERDET'in mevcut yöntemlere göre daha başarılı olduğu ve GPS aldatma saldırılarını etkili bir şekilde tespit edebildiği belirlenmiştir. Bu çalışma, algı verilerine dayalı makine öğrenmesi tabanlı yaklaşımların GPS aldatma saldırılarını tespit etmede etkili bir yol olduğunu göstermektedir.

Ali Broumadan belgesinde [71] aldatma taktiklerine karşı koymak amacıyla, GNSS alıcısının sinyal işleme zincirinin farklı aşamalarında geliştirilen ve test edilen çeşitli tespit yöntemleri bulunmaktadır. Yazarlar, bu yöntemlerin statik ve dinamik koşullar altında hem donanım simülasyonları hem de yazılım tabanlı aldatma senaryoları kullanılarak değerlendirildiğini belirtmektedir. Testlerde, HackRF gibi cihazlarla yapılan yazılım tabanlı aldatma yöntemleri ve yüksek hassasiyetli alıcılar kullanılarak yapılan donanım simülasyonları yer almaktadır. Aldatma saldırılarını tespit etmek için kullanılan çeşitli metrikleri ve bu metriklerin nasıl işlediğini detaylandırmaktadır. Örneğin, giriş gücü analizi, yapısal güç içerik analizi, etkili C/N0, sinyal kalitesi izleme (SQM) ve saat izleme gibi yöntemler kullanılmaktadır. Giriş gücü analizi, alıcıya eklenen interferans sinyalleri ile giriş gücündeki artışı izleyerek saldırıları tespit etmeyi amaçlar. Yapısal güç içerik analizi ise GNSS sinyallerinin döngüsel istasyonerliğinden yararlanarak, alınan örnek setindeki aşırı yapılandırılmış sinyal

gücünü tespit eder. SQM metrikleri, özgün ve aldatma sinyallerinin etkileşimi sonucu ortaya çıkan korelasyon zirvesi şekil bozulmalarını tespit eder. Saat izleme ise tek anten kaynağından gelen aldatma sinyallerini, hareketli bir alıcının konum çözümlemesi temelinde tespit eder. Bu tespit yöntemlerinin farklı aldatma ve aldatma olmayan senaryolar altında performanslarını değerlendirmişlerdir. Test sonuçları, aldatma sinyallerinin tespit edilmesinde bu metriklerin ne kadar etkili olduğunu göstermektedir. GNSS alıcıları için gerçek zamanlı bir aldatma tespit birimi, bu metrikleri toplayarak analiz etmekte ve her iki saniyede bir alıcının aldatma saldırısı altında olup olmadığını belirlemektedir. Tespit birimi, jamming ve çoklu yol sinyallerinin varlığında yanlış tespit olasılığını azaltmayı ve aldatma saldırılarını yüksek bir güvenle tespit etmeyi amaçlamaktadır.

GPS aldatma tespit yöntemleri genellikle doğrudan alıcının parametrelerine dayanmaktadır, bu parametreler arasında Doppler shift, SNR, güç gibi faktörler bulunmaktadır [58]. Ancak, bu yöntemler genellikle keskinliğe odaklanmıştır, tespit hızı kadar kesinlik de önemlidir. Bu makale, aldatma sinyalinin algılanmasının hızına odaklanarak, en hızlı tespit yöntemini araştırmaktadır. İlk olarak, iki bağımsız düşük maliyetli GPS alıcısına bağlanmış monopol-paçalı hibrit bir anten önerilmektedir. Bu anten, iki alıcıya gelen GPS sinyallerini besler ve bu sinyallerin taşıyıcı-sinyal-gürültü oranı (C/No) farkları en hızlı tespit algoritması için bir istatistik olarak kullanılır. Bu algoritma, C/No istatistiksel ölçüm çıktısına dayanarak aldatma saldırısının ne zaman gerçekleştiğini tespit etmek için uygulanır. Bir donanım test platformu kullanılarak GPS aldatma saldırısı simüle edilmiş ve gerçek GPS sinyalinin C/No'su ile sahte GPS sinyalinden gelen C/No'nun olasılık dağılımı elde edilmiştir. Analiz sonuçları, önerilen en hızlı tespit algoritmasının, GPS aldatma saldırısının gerçekleştiği anda etkili bir şekilde tespit edilebileceğini göstermektedir.

Caparra ve Laurenti tarafından yapılan çalışma [72], Kod Kaydırma Anahtarlama (Code Shift Keying, CSK) modülasyonunun küresel navigasyon uydu sistemlerinde (GNSS) menzil sinyallerinin doğrulanması için bir mekanizma olarak potansiyelini araştırmaktadır. CSK'nın kullanılabilirliği, avantajları ve dezavantajları tartışılmış, mevcut tespit algoritmalarına rakip olabileceği veya entegre edilebileceği üzerinde durulmuştur. Ayrıca, CSK'nın SCER (Security Code Estimation and Replay) GPS aldatma saldırısı

altında performansı incelenmiştir. CSK'nın M-ary yıldız işaretine sahip olması, sembol tahminini karmaşık hale getirebilirken, saldırganlar için meşru sinyallerden ayırt edilmesi zor sinyaller üretebilme potansiyelini göstermiştir. Çalışma, CSK'nın Spreading Code Encryption (SCE) ile birleştirilmesi olasılığını da ele almış, güvenlik avantajlarına rağmen alıcı işleme karmaşıklıklarına dikkat çekmiştir. Gelecek araştırma önerileri arasında, performansın gerçekçi kanal modellerinde değerlendirilmesi, kanal bozulmalarına karşı direncin artırılması ve CSK'nın diğer modülasyon şemalarıyla karşılaştırılması yer almaktadır.

Gao ve Li'nin çalışması [61], küresel navigasyon uydu sistemlerinin (GNSS) ölçüm ve navigasyon kullanıcılarının, yerleşim, navigasyon ve zaman (PNT) hizmeti olmadan çalışamayacağını, ancak kullanıcıların öngörülemeyen ve karmaşık müdahalelerle ve hatta yanıltma ile karşılaştığını belirtmektedir. Özellikle, insansız hava araçlarının (UAV) güvenliğe tehdit oluşturması durumunda GNSS yanıltma teknolojisinin etkili bir şekilde kontrol edilmesi ve hatta karşılanması için önemli bir araç olduğunu vurgular. Çalışma, mevcut yanıltma algoritmalarının yanı sıra navigasyon sistemi yapılandırması ve uçuş kontrol prensiplerini dikkate alarak, donanmış bir UAV'nin GNSS yanıltma ortamında nasıl tepki vereceğini ve gizli yönlü yanıltma gerçekleştirmek için bir algoritma önerir. Önerilen algoritma, bir sabit noktalı dört adımlı yanıltma stratejisi içerir ve UAV'nin LSR-RAIM'inden kaçınmaya dikkat eder. Deneysel analizler, algoritmanın etkinliğini ve gizliliğini doğrulamış, GNSS gizli yönlü yanıltmanın etkin bir şekilde gerçekleştirilebileceğini göstermiştir. Önerilen algoritmanın, gerçek yanıltma senaryolarına uygulanabileceği ve gelecek araştırmaların, daha duyarlı ve etkili karşı tedbir teknikleri ile donatılmış UAV'lerin etkisini incelemeye odaklanacağı belirtilmektedir. Bu çalışma ayrıca, GNSS aldatmaya karşı tedbirlerle donatılmış bir IMU'ya sahip insansız hava aracı üzerinde GNSS aldatma deneylerini içermektedir. Dört aşamalı bir aldatma algoritması tasarlanmış ve uygulanmıştır. Aldatma sırasında LSR-RAIM gibi aldatma tespit yöntemlerinin başarısız olduğu gözlemlenmiştir.

Tae-Hee Kim'in makalesi [62], GPS aldatmaca sinyallerinin çeşitli tiplerini ve etkilerini azaltma stratejilerini incelemektedir. Özellikle, sahte GNSS sinyallerinin meşru olanlarla

senkronize edildiği orta düzeydeki aldatmacalara odaklanmaktadır. Aldatmacayı tespit etmek için, mutlak ve göreceli GNSS sinyal gücü, sinyal gücü değişim oranı ve aralık oranları gibi faktörler analiz edilmektedir. Hilelemenin önlenmesi yöntemleri, sinyal işleme yoluyla aldatmaca kanallarının ortadan kaldırılmasını ve RF faz kontrolü aracılığıyla aldatmaca sinyallerinin dengelenmesini içermektedir. Simülasyonlar, GNSS sinyal jeneratör yazılımı kullanılarak gerçekleştirilmiş ve aldatmaca sinyalleri oluşturulup aldatmaca karşıtı sinyallerle dengelenmiştir. Sonuçlar, aldatmaca tarafından tetiklenen anormal navigasyon çözümlerinden aldatmaca karşıtı önlemlerle normal çözümlere geçişin izlerini takip döngüsü hatalarında ve yarıçapındaki değişikliklerde göstererek ortaya koymaktadır. Gelecekteki araştırmalar, GPS alıcılarının RF-Front End'inde aldatmacayı önleme tekniklerinin geliştirilmesine odaklanacaktır.

GNSS sinyallerinin aldatılması, konum ve zaman çözümü oluşturmak için yanıltıcı verilerin bilinçsiz kullanımı nedeniyle can güvenliği uygulamaları kullanan kullanıcılara sürekli bir tehdit oluşturur [63]. Bu tehdide karşı, sinyal işleme aşamalarında uygulanan anti-aldatmaca teknikler arasında, potansiyel olarak aldatılmış GNSS sinyallerini tespit etmek için denetimli makine öğrenimi tabanlı bir yaklaşım önerilmektedir. Bu yaklaşım, çapraz-korelasyon izleme yöntemiyle birden fazla GNSS gözlemlenebilir ve ölçülebilirin çapraz korelasyon verilerini girdi olarak kullanmaktadır. Hem laboratuvarda üretilen sentetik hem de gerçek dünya aldatmaca veri setleri üzerinde yapılan testler, denetimli makine öğrenimi algoritmalarının GNSS aldatmacasını tespit etme yeteneğini göstermektedir. Özellikle, kullanılan destek vektör makineleri (Support Vector Machine, SVM) yönteminin, aldatma sinyallerini tespit etme kapasitesinin yüksek olduğu gözlemlenmiştir. Bu çalışma, GNSS çekirdek takımlarının sürekli olarak ilgi gören konum-navigasyon-zaman (Position-Navigation-Time, PNT) uygulamalarında, sinyal aldatmasına karşı savunmasızlığı göz önünde bulundurarak önemli bir ilerleme sağlamaktadır.

Yang'ın çalışması [64], GNSS aldatma tespitinden sonra "aldatma korelasyon tepe iptali (Aldatma correlation peak cancellation, SCPC)" yöntemiyle gerçek GNSS sinyaline ulaşmayı hedeflemektedir. Bu yöntem, pahalı donanımlar gibi çok kanallı anten dizilerine dayanır ve aldatma iptali için aldatma sinyalinin genlik ve fazlarının tahmin edilip karşı

sinyalle iptal edilmesini içerir. Farklı olarak, diğer aldatma sinyali iptal çalışmalarından, filtreleme yöntemi yerine sinyalin uygun bölgelerindeki korelasyonlarına bakarak aldatma sinyali tespiti yapılarak iptal sinyallerinin üretilmesi önerilir. TEXBAT verileri üzerinde yapılan testler, önerilen yöntemin etkili olduğunu göstermiştir. Bu yaklaşımda, GNSS aldatma saldırılarının korelasyon tepe bölgesinde tespit edilip tanımlandığı ve sahtecilik sinyali parametrelerinin tahmin edilerek ters iptal akışının oluşturulduğu bir yöntem sunulmaktadır. Önerilen şema, GNSS sahteciliğini bastırmak için etkili ve uygun bir çözüm sunmaktadır.

Schmidt'in çalışması [65], tek antenli alıcılar için bir küresel navigasyon uydu sistemi (GNSS) sahtecilik tespit ve sınıflandırma tekniği önermektedir. Bu teknikte, En Küçük Mutlak Küçülme ve Seçim Operatörü (Least Absolute Shrinkage and Selection Operator, LASSO) kullanılarak temel bant korelatör alanında bir optimizasyon problemi formüle edilir. Alınan sinyalin korelatör çıktılarını bir sözlük oluşturmak için üçgen şekilli işlevlerden oluşan bir modellemeye dönüştürülür ve seyrek sinyal işleme kullanılarak sözlükten kaydırılmış eşleşen üçgenlerin bir ayrışımı seçilir. Bu minimizasyon problemi, optimal çözümü seyrek vektör çıktısında iki farklı kod-faz değerinin (otantik ve sahtecilik) bir ayrışımını gözlemleyerek potansiyel bir sahtecilik saldırı tepe noktasının varlığını ayırt eder. Yanlış alarmları azaltmak için bir eşik değeri kullanılır. Ayrıca, sözlüğü kaydırılmış üçgenlere daha yüksek çözünürlüklü bir şekilde genişleterek minimizasyon problemine bir varyasyon sunulur. Önerilen teknik, sahteciliği bastırmaya yardımcı olan gelişmiş bir ince kazanç izleme aracı olarak uygulanabilir. Yapılan deneyler, sentetik veri simülasyonlarından ve gerçek bir veri kümesi olan Texas sahtecilik test pilinden otantik ve sahteci tepe noktalarını ayırt edebildiğini göstermektedir. Önerilen yöntem, nominal sinyal-gürültü oranı koşullarında ve otantik-sahteci güç farkının 3 dB olduğu durumlar için %0,3 hata oranı elde etmektedir.

Ahmad'ın çalışmasında [73], GPS sinyallerinin bant içi girişimlere karşı duyarlı olduğu vurgulanarak, GPS alanındaki sahtecilik ve karşı-sahtecilik tekniklerinin ortaya çıkan endişeleri ele alınmaktadır. Giriş, modern navigasyon sistemlerinde GPS'in yaygın rolünü ve kasıtlı ve kasıtsız müdahalelere karşı duyarlılığını vurgulamaktadır. Makale, sahtecilik

saldırılarının karmaşıklıklarını aydınlatarak, eşzamanlı ve eşzamanlı olmayan yöntemler arasında ayrım yapar ve GPS alıcılarının zayıflıklarının aşamalarını ve olası karşı önlemleri keşfeder. Sahtecilik tespit ve azaltma tekniklerinin kapsamlı bir araştırması, GPS sahteciliğiyle başa çıkmanın karmaşıklığını vurgular ve etkili ancak hesaplama açısından verimli karşı-sahtecilik stratejilerinin gerekliliğini vurgular. Bu bağlamda, aldatma sinyallerinin tespit edilmesi ve karşı önlemler üzerine önerilerde bulunulmuş ve yapılan testler sunulmuştur.

Guo ve arkadaşları çalışmalarında [74], GPS/inerisyal-navigasyon-sistemi entegreli bir insansız hava aracının (UAV) gizli sahtecilik algoritması incelenmektedir. Önerilen algoritma, sahte GPS sinyalinin ivme bileşeninin, UAV'nin mevcut ivmesi ile sahtecilik kontrol girişi arasındaki fark olduğunu teorik olarak kanıtlamaktadır. Bu algoritma, GPS sahtecilik saldırıları sırasında uçuşunu değiştirmesinden kaynaklanan olumsuz sonuçlardan kaçınmak için, sahtecilik trajektorisinin referans trajektöre göre yavaşça değişmesini gerektirir. Benzetim sonuçları, önerilen gizli sahtecilik algoritmasının doğruluğunu doğrulamış ve aldatma trajektorisi planlaması dikkate alındığında, sahtecilik etkisinin daha belirgin hale geldiğini göstermiştir. Bu yaklaşım, GPS aldatma tespiti ve karşı önlemler konusunda önemli bir katkı sağlamaktadır.

Lin'in çalışması [75], düşük doğruluk hassasiyetine sahip bir GPS alıcısının frekans doğruluğunu artırmak için bir yöntem sunmaktadır, özellikle düşük doğrulukta osilatörlere sahip platformlar için hedeflenmektedir. GPS sabitlemelerinin genellikle hassas yerel osilatör frekanslarına dayandığını göz önüne alarak, önerilen frekans kalibrasyon yöntemi, uydu edinimi sırasında frekans arama aralığını daraltmayı amaçlamaktadır. Bu yöntemi, düşük doğruluklu bir osilatöre sahip bir PlutoSDR transceiver üzerinde uygulayarak, yazarlar HDOP 2.4'ü olan bir konumlandırma hassasiyeti sağlayan bir dış mekân GPS sabitlemesi gerçekleştirdiler. Bu yaklaşım, düşük doğruluklu osilatörlere sahip SDR'lerle başarılı GPS konumlandırmanın zorluğunu ele alırken, GPS uygulamalarında SDR platformlarının işlevselliğini genişletmek için maliyet etkin bir çözüm sunar.

Fazör ölçüm birimi (Phase Measurement Unit, PMU) ölçümlerini önemli ölçüde değiştiren

bir sahtekarlık saldırısı şebekenin normal çalışmasını ciddi şekilde etkileyebilir. Bu soruna yanıt olarak Risbud ve arkadaşları, ağ durumu tahmini ve saldırı yeniden yapılandırma problemini konveks olmayan kısıtlı en küçük kareler problemine dönüştürmek için sahtekarlık saldırısı metrik modelini kullanmıştır [76]. Tanımlama ağındaki en savunmasız fazör ölçüm biriminin optimize edilmesi gerektiğinden, ortak durum tahmini ve saldırı yeniden yapılandırma etkileşimi minimizasyon algoritması, sahtekarlık saldırısına yanıt veren sorunu çözmek için kullanılır. Sinyal işleme teknolojisi aldatmanın etkilerini azaltabilir. Kimetal. sinyal işleme ile sahte kanalları ortadan kaldırmak için bir yöntem önermiştir [62]. Araştırma ekibi ayrıca radyo frekansı faz kontrolü ile sahtekarlık sinyalinin ortadan kaldırılması için bir sahtekarlık bastırma yöntemi önermiştir. Bu iki yöntem, navigasyon konumlandırma sonucunun sahtecilik sinyalinin neden olduğu anormal durumdan normal duruma dönüştürülmesine neden olur. Berardo ve arkadaşları sinyal işleme teknolojisi ile birleştirilmiş bir zaman atlamalı (time jumping, TJ) sahteciliğe karşı sinyal işleme algoritması önermiştir [77]. Şema, çoklu yolu tespit etmek için giriş sinyali ile yerel kopya arasındaki korelasyon fonksiyonunu gözlemlemek için çoklu korelatör kullanma fikrine dayanmaktadır. Gerçek sinyaller ve sahtekarlık sinyalleri arasındaki göreceli gecikmenin tahmin edilmesi, alıcının kilidi kaybetmesine ve gerçek sinyale yeniden kilitlenmesine neden olur. Artık sinyalin etkisi nedeniyle, sahteciliği bastıran navigasyon sinyali ile elde edilen konumsal doğruluk, gerçek sinyal ile elde edilen navigasyon konumlandırma pozisyonundan biraz daha düşüktür.

Bhamidipati ve arkadaşları, yaygın olarak dağıtılmış bir statik alıcıya ve bilinen konum ağına dayalı bir zaman doğrulama algoritması önermiştir [78]. İlk olarak, koşullu olarak kısıtlanmış dört fazlı taşıyıcı silme giriş sinyali üzerinde çift yönlü bir çapraz korelasyon işlemi gerçekleştirilir ve yardımcı konum bilgisi, farklı alıcı uçlar tarafından alınan P(Y) kodunun beklenen zaman ofsetini tahmin etmek için kullanılır. Yukarıdaki işlemlere dayanarak, her alıcı, her alıcının ve ortak uydusunun eşleştirilmiş çapraz korelasyon tepe ofsetinin ve genliğinin ağırlıklı toplamı analiz edilerek doğrulanır. Wang ve arkadaşları, alıcı yakalama aşamasında eşiğin üzerinde bulunan korelasyon tepe noktalarının sayısına dayalı bir sahtekarlık sinyali olup olmadığına karar vermek için yeni bir yöntem önermiştir [78].

İki korelasyon tepesi bulunursa, sahtekarlık sinyali olduğunu gösterir; bir tepe bulunursa, yalnızca kaba sinyal / gürültü oranı güç eşiğinden daha az olduğunda ve korelasyon fonksiyonu genişliği genişlik eşiğinden daha az olduğunda, sahtekarlık sinyali olmadığını gösterir. Yöntem, gerçek sinyal ile sahtekarlık sinyalinin çakışması sorununu çözebilir. Yukarıdaki güç eşiğinin teorik hesaplama yöntemi ve nicel referans değeri verilmiş, etkileyen faktörler ve performans analiz edilmiştir.

Farklı uydularla ilişkilendirilen ve aynı kablosuz kanal üzerinden yayılan sahte uydu sinyallerinin oranı yüksek korelasyonlu iken, bağımsız kablosuz kanallar üzerinden iletilen gerçek sinyal oranları birbirinden bağımsızdır. Bu nedenle, sahtekarlık saldırıları bu oranların korelasyonu ile tespit edilebilir. Yukarıdaki temel prensiplere göre, Li ve arkadaşları kablosuz kanallardaki çoklu yollar arasındaki gecikme ve kazanç oranını kullanarak sahtekarlık tespiti için yeni bir yöntem önermektedir [46]. Khalajmehrabadi ve arkadaşları statik GPS alıcıları için zaman senkronizasyonu saldırı reddi ve azaltma (time synchronization attack rejection and mitigation, TSARM) tekniğini ve değerlendirme yöntemini önermişlerdir [79]. Yöntem, sahteciliğin etkisini azaltmak için pratikliği incelemek için TEXBAT'ta bulunan gerçek uydu sinyali sahteciliği mekanizmasının değerlendirme platformunu kullanır. Teknik, kurban hedef alıcıda ölçülen pseudorange oranını kullanır ve anormal davranışını değerlendirir. Ölçülen değeri, gerçek aldatıcı tarafının gerçek kısıtlamalarını dikkate alarak düzeltir. Carson ve arkadaşları bir GPS sahtekarlığı tespit ve giderme algoritması önermiştir [80]. Han ve arkadaşları, sahtekarlık ve parçacık ağırlıkları arasındaki ilişkiyi kullanan parçacık filtresi (particle filter, PF) tabanlı bir maksimum parçacık ağırlığı sahtekarlık tespit şeması önermiştir [81]. Yöntem, geliştirilmiş bir sağlam tahmin yöntemi kullanarak ve anormal maksimum parçacık ağırlığını yakalayarak sahteciliği tespit eder ve bastırır.

Shang ve arkadaşları, aldatıcının konumunu izlemek için alıcıyı kullanmak üzere bir yöntem önermiştir. Yöntem, sahte sinyali yeniden oynatmak için alıcı tarafından alınan sahte uydu sinyalinin zaman ve efemeris parametrelerini kullanır ve böylece aldatıcıyı izleme etkisini elde eder [82].

Wesson ve arkadaşları, simetrik diferansiyel otokorelasyon bozulma izleme ve bant içi güç

izlemeyi düşük bir yanlış alarm olasılığı ile birleştiren sahtecilik tespit yöntemi önermiştir [83]. Gao ve arkadaşları, ara sahtekarlık saldırganlarını kullanarak sahtekarlık saldırılarının zayıflıklarını belirlemek için taşıyıcı faz ve kod fazı tutarlılığının tespitine dayanan bir sahtekarlık önleme yöntemi önermiştir [84].

4 GPS ALDATMA VE KARŞI TEDBİR YÖNTEMLERİNİN GERÇEK ZAMANLI SİSTEMLER ÜZERİNDE KARŞILAŞTIRILMASI

Önceki bölümde detaylı olarak bahsedilen GPS aldatma ve karşı tedbir yöntemlerinin farklı parametrelere göre karşılaştırılması yapılarak en uygulanabilir veya en etkili yöntemin tespiti yapılmaya çalışılmıştır.

Bu çalışmada yöntemlerin karşılaştırılması literatürde geçen parametrelere, şimdiye kadar yapılan çalışmalardaki sonuçlara ve bu tez kapsamında gerçeklemesi yapılan yöntemler üzerinden değerlendirilmiştir.

4.1 Literatürde GPS Aldatma ve Karşı Tedbir Yöntemlerinin Karşılaştırılması

Literatürde, çeşitli GPS aldatma teknikleri ve bu saldırılara karşı geliştirilen çok sayıda savunma yöntemi detaylı olarak incelenmiştir. Özellikle Psiaki ve Humphreys [9] tarafından yapılan araştırmalar, GPS aldatma tekniklerinin sınıflandırılması ve karşı tedbirlerin etkinliğinin değerlendirilmesi konusunda önemli katkılar sağlamıştır. Benzer şekilde, Wu ve diğerleri [4] tarafından yapılan kapsamlı çalışmalar, GPS aldatma ve Karşı Tedbir teknolojilerini hem sinyal seviyesi hem de veri seviyesi perspektifinden ele alarak derinlemesine analiz etmiştir. Bu çalışmalar sırasında, maliyet, uygulama zorluğu, tespit olasılığı ve güvenilirlik gibi parametreler göz önünde bulundurulmuştur. Bu bölümde, literatürde belirtilen GPS aldatma yöntemleri ile karşı tedbir tekniklerini bu parametreler ışığında karşılaştırarak, mevcut yaklaşımların etkinliğini ve uygulanabilirliğini değerlendirmeyi amaçlamaktadır. Tablo 4.1'de aldatma yöntemleri ve Tablo 4.2'de karşı tedbir yöntemleri verilmiştir.

Aldatma Teknikleri	Açıklama
Meaconing [9], [20], [82]	GNSS sinyallerini alıp gecikmeli olarak yeniden yayınlama
Replay Attack [9], [18], [26]	Kaydedilmiş GNSS sinyallerini yeniden oynatma
Signal Simulation [4], [17]	GNSS sinyallerini taklit eden sahte sinyaller üretme
Nulling [4], [9], [50]	Orijinal GNSS sinyallerini engelleyip sahte sinyaller gönderme
SCER Attack [4], [18], [65]	Güvenlik kodlarını tahmin ederek sinyalleri yeniden oynatma

Tablo 4.1 Kullanılan GNSS Aldatma Yöntemleri

Karşı Tedbir Teknikleri	Açıklama
Pseudorange Tabanlı RAIM [4], [9], [69]	GNSS sinyallerinin doğruluğunu kontrol eden yöntem
Doppler Shift Monitoring [31], [33], [42]	Sinyal frekansındaki kaymaları izleme
Signal Quality Monitoring [47], [56], [57]	Sinyal kalitesini değerlendirme
Güç İzleme [28], [44], [62]	Sinyal gücünü kontrol etme
Korelasyon Fonksiyonu Bozulma İzleme [39], [45] [47]	Sinyal korelasyon fonksiyonundaki bozulmaları izleme
Sapma İzleme [9], [29], [66]	Sinyal sapmalarını takip etme
NMA [9], [72]	Navigasyon mesajlarının doğruluğunu kontrol etme
IMU ve Saat İzleme [48], [79], [85]	Atalet ölçüm birimi ve saat takibi ile doğrulama
Çoklu Anten [30], [50]	Birden fazla anten kullanarak sinyalleri doğrulama

Tablo 4.2 Kullanılan GNSS Karşı Tedbir Yöntemleri

İncelenen çalışmalar sonucunda, GPS aldatma saldırılarına karşı kullanılan karşı-tedbir tekniklerinin performanslarını değerlendiren detaylı bir tablo oluşturulmuştur. Bu tablo aşağıda Tablo 4.3 olarak verilmiştir. Tabloda yer alan aldatma yöntemleri arasında Meaconing, Replay Attack, Signal Simulation, Nulling ve SCER (Security Code Estimation and Replay) Saldırısı bulunmaktadır. Her bir aldatma yöntemine karşı kullanılan karşı-tedbir teknikleri, maliyet, tespit olasılığı ve güvenilirlik parametreleri açısından incelenmiştir. Maliyet, bir tekniğin uygulanma maliyetini düşük, orta veya yüksek olarak belirtirken; tespit olasılığı, bir tekniğin aldatma saldırılarını tespit etme kapasitesini düşük, orta veya yüksek olarak ifade eder. Güvenilirlik ise, tekniğin güvenilirliğini aynı şekilde düşük, orta veya yüksek olarak değerlendirir. Bu parametreler, karşı-tedbir tekniklerinin etkinliğini ve uygulanabilirliğini belirlemek için kritik öneme sahiptir ve GPS aldatma saldırılarına karşı hangi tekniklerin en etkili olduğunu ortaya koymak için kullanılmıştır. Tabloda yer alan karşı-tedbir teknikleri arasında Pseudorange Tabanlı RAIM (Receiver Autonomous Integrity Monitoring), Doppler Shift Monitoring, Signal Quality Monitoring, Güç İzleme, Korelasyon Fonksiyonu Bozulma İzleme, Sapma İzleme, NMA (Navigation Message Authentication), IMU (Inertial Measurement Unit) ve Saat İzleme ile Çoklu Anten yöntemleri bulunmaktadır. Bu yöntemler, ilgili aldatma tekniklerine karşı farklı performans seviyeleri sergilemekte

olup, çalışmanın sonuçları doğrultusunda en uygun karşı tedbirlerin seçilmesine yardımcı olmaktadır.

Aldatma Yöntemi	Karşı Tedbir Tekniği	Maliyet	Tespit Olasılığı	Güvenilirlik
Meaconing [9], [20], [82]	Pseudorange Tabanlı RAIM [4], [9], [69]	Düşük	Orta	Orta
	Doppler Shift Monitoring [31], [33], [42]	Orta	Yüksek	Yüksek
	Signal Quality Monitoring [47], [56], [57]	Orta	Düşük	Orta
	Güç İzleme [28], [44], [62]	Düşük	Düşük	Düşük
	Korelasyon Fonksiyonu Bozulma İzleme [39], [45], [47]	Yüksek	Yüksek	Yüksek
	Sapma İzleme [9], [29], [66]	Orta	Orta	Yüksek
	NMA [9], [72]	Düşük	Yüksek	Yüksek
	IMU ve Saat İzleme [48], [79], [85]	Yüksek	Yüksek	Yüksek
	Çoklu Anten [30], [50]	Yüksek	Yüksek	Yüksek
Replay Attack[9], [18], [26]	Pseudorange Tabanlı RAIM [4], [9], [69]	Düşük	Orta	Orta
	Doppler Shift Monitoring [31], [33], [42]	Orta	Yüksek	Yüksek
	Signal Quality Monitoring [47], [56], [57]	Orta	Düşük	Orta
	Güç İzleme [28], [44], [62]	Düşük	Düşük	Düşük
	Korelasyon Fonksiyonu Bozulma İzleme [39], [45], [47]	Yüksek	Yüksek	Yüksek
	Sapma İzleme [9], [29], [66]	Orta	Orta	Yüksek
	NMA [9], [72]	Düşük	Yüksek	Yüksek
	IMU ve Saat İzleme [48], [79], [85]	Yüksek	Yüksek	Yüksek
	Çoklu Anten [30], [50]	Yüksek	Yüksek	Yüksek
Signal Simulation [4], [17]	Pseudorange Tabanlı RAIM [4], [9], [69]	Düşük	Düşük	Orta
	Doppler Shift Monitoring [31], [33], [42]	Orta	Orta	Orta
	Signal Quality Monitoring [47], [56], [57]	Orta	Yüksek	Yüksek
	Güç İzleme [28], [44], [62]	Düşük	Düşük	Düşük
	Korelasyon Fonksiyonu Bozulma İzleme [39], [45], [47]	Yüksek	Yüksek	Yüksek
	Sapma İzleme [9], [29], [66]	Orta	Orta	Yüksek
	NMA [9], [72]	Düşük	Yüksek	Yüksek
	IMU ve Saat İzleme [48], [79], [85]	Yüksek	Yüksek	Yüksek
	Çoklu Anten [30], [50]	Yüksek	Yüksek	Yüksek
Nulling [4], [9], [50]	Pseudorange Tabanlı RAIM [4], [9], [69]	Düşük	Düşük	Orta
	Doppler Shift Monitoring [31], [33], [42]	Orta	Orta	Orta
	Signal Quality Monitoring [47], [56], [57]	Orta	Düşük	Orta
	Güç İzleme [28], [44], [62]	Düşük	Düşük	Düşük
	Korelasyon Fonksiyonu Bozulma İzleme [39], [45], [47]	Yüksek	Yüksek	Yüksek
	Sapma İzleme [9], [29], [66]	Orta	Orta	Yüksek
	NMA [9], [72]	Düşük	Yüksek	Yüksek
	IMU ve Saat İzleme [48], [79], [85]	Yüksek	Yüksek	Yüksek
	Çoklu Anten [30], [50]	Yüksek	Yüksek	Yüksek
SCER Attack[4], [18], [65]	Pseudorange Tabanlı RAIM [4], [9], [69]	Düşük	Düşük	Orta
	Doppler Shift Monitoring [31], [33], [42]	Orta	Orta	Orta
	Signal Quality Monitoring [47], [56], [57]	Orta	Orta	Orta
	Güç İzleme [28], [44], [62]	Düşük	Düşük	Düşük
	Korelasyon Fonksiyonu Bozulma İzleme [39], [45], [47]	Yüksek	Yüksek	Yüksek
	Sapma İzleme [9], [29], [66]	Orta	Orta	Yüksek
	NMA [9], [72]	Düşük	Yüksek	Yüksek
	IMU ve Saat İzleme [48], [79], [85]	Yüksek	Yüksek	Yüksek
	Çoklu Anten [30], [50]	Yüksek	Yüksek	Yüksek

Tablo 4.3 GNSS Aldatma ve Karşı Tedbir Tekniklerinin Karşılaştırılması

Bu tez kapsamında yapılan çalışmalardan farklı olarak teorik olarak incelenmiş ve literatürde yer edinmiş GPS aldatma ve karşı tedbir yöntemlerinden gerçeklenebilir olanları gerçek sistemler üzerinde denenerek aldatılma süresi, mesafe performans analizi gibi parametrelere göre karşılaştırılacaktır.

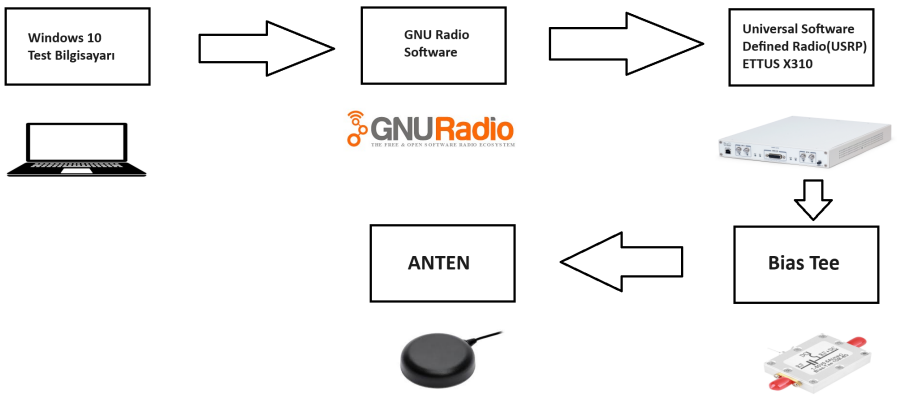
4.2 GPS Aldatma Yöntemlerinin Gerçeklenmesi

Bu bölümde, GPS aldatma yöntemlerinin nasıl gerçeğe dönüştürüldüğü incelenecektir. GNSS verilerinin toplanması veya oluşturulması ve bu verilerin kullanılarak çeşitli deneylerin gerçekleştirilmesi üzerinde durulacaktır.

4.2.1 GNSS Verilerinin Toplanması

GNSS verilerine ulaşmak için 3 farklı yöntem kullanılmıştır. Bu yöntemler USRP ile gerçek I-Q veri toplanması, GPS-SDR-SIM kütüphanesi ile GPS L1 C/A GPS sinyallerinin üretilmesi ve TEXBAT kütüphanesidir.

4.2.11. USRP ile Gerçek GNSS Sinyal Toplanması Sabit bir konumunda Ettus x310 USRP cihazına yüksek kazançlı aktif anten bağlanılarak GNSS verilerinin I-Q veriler şeklinde kaydedilmesi sağlanmıştır. Bu işlem sırasında GNU Radio Software yazılımı kullanılmıştır.



Şekil 4.1 USRP ile Veri Toplama Sistem Modeli

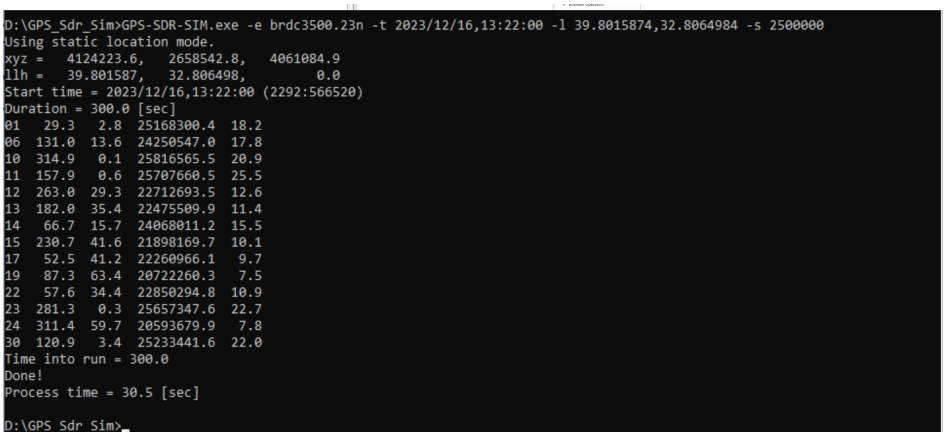
Şekil 4.1'de gösterildiği gibi GNSS verilerinin düzgün bir şekilde toplanılabilmesi için açık bir araziye, test bilgisayarına, USRP cihazına, Bias Tee ye ve aktif antene ihtiyaç vardır.

Test bilgisayarı GNU Radio Companion yazılımını kullanarak USRP cihazını ethernet hattı üzerinden kontrol etmektedir. Bias tee yardımıyla aktif edilmiş yüksek kazançlı anten USRP cihazının RX girişine bağlanmıştır. Kullanılan yazılım sayesinde anten üzerine düşen GNSS yayınları görsel olarak izlenmiş ve daha sonra yayınlanmak üzere I-Q veriler olarak kaydedilmiştir.

Bias tee, elektronik ve RF mühendisliğinde kullanılan bir cihaz olup, DC sinyali AC sinyaliyle birleştirmek veya ayırmak için kullanılır. Üç bağlantı noktasına sahiptir: RF Portu (yalnızca AC sinyalleri), DC Portu (yalnızca DC sinyalleri) ve Common Port (her iki sinyalin birleştirildiği veya ayrıldığı port). Bias tee, yüksek frekanslı AC sinyallerin DC bileşenlerinden ayrılmasını veya birleştirilmesini sağlar, böylece antenler, amplifikatörler ve telekomünikasyon cihazları gibi uygulamalarda kullanılır. Bu sayede, RF sinyalleri bozulmadan iletilirken, DC güç sağlanabilir ve RF devrelerinde performans kaybı olmadan çalışılabilir. Burada bias tee aktif antenin içindeki amfiyi aktif etmek ve kazancını arttırmak için kullanılmıştır.

4.2.12. GPS-SDR-SIM kütüphanesi ile GPS L1 Verisi Üretilmesi GPS-SDR-SIM, açık kaynaklı bir yazılım tabanlı radyo simülatörü olup, Global Konumlama Sistemi sinyallerinin simülasyonunu gerçekleştirmek amacıyla kullanılmaktadır. GNU General Public License (GPL) altında dağıtılan bu kütüphane, kullanıcıların gerçek GPS sinyallerini taklit eden sinyaller oluşturmasını sağlayarak, GPS alıcılarının performansını test etme ve değerlendirme imkanı sunmaktadır. GPS-SDR-SIM, GPS alıcıları için laboratuvar testleri, eğitim projeleri ve araştırma çalışmaları gibi çeşitli alanlarda geniş bir kullanım yelpazesi sunmaktadır. Komut satırı tabanlı arayüzü, kullanıcıların belirli bir yörünge veya konum için GPS sinyalleri üretmesine olanak tanımakta ve yüksek doğruluk ve hassasiyet sağlamaktadır; bu da güvenilir test sonuçları elde edilmesine katkı sağlamaktadır. Bu kütüphane, yeni geliştirilen GPS alıcılarını laboratuvar ortamında test etmek, GPS sinyal işleme ve navigasyon sistemleri üzerine eğitim vermek ve GNSS araştırmaları yapmak gibi çeşitli kullanım senaryolarına sahiptir.

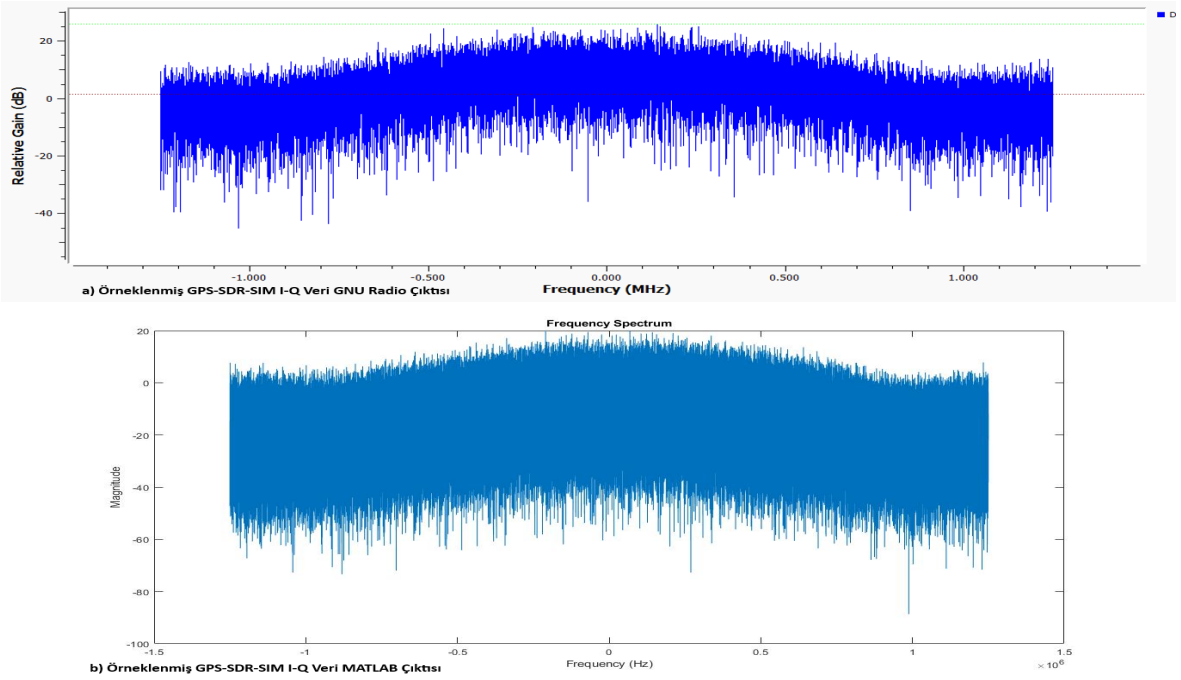
Bu simülasyon kütüphanesi, onaltılık sayı biçiminde sayısal GPS sinyali (I-Q verileri) oluşturmaktadır. GPS-SDR-SIM en az iki girdi ile çalışmaktadır. İlk girdi RINEX navigasyon dosyasıdır ve diğer girdi ise aldatma yapılmak istenen konum bilgisidir. NASA tarafından sağlanan RINEX navigasyon dosyası açık kaynak olarak paylaşılmaktadır [86]. Ayrıca Yayın Efemerisi (Broadcast Ephemeris, BRDC) dosyası olarak da adlandırmaktadır. Bu dosya her güne ait GPS uydu navigasyon verilerinden oluşmaktadır. Bu navigasyon verileri, GPS alıcılarının kullanıcı konumunu hesaplamak için önceden bilgi edinebilmelerini sağlayacak şekilde her bir uydunun kesin konumunu içermektedir. Bu yöntemde, GPS L1 sinyallerinin matematiksel modellemesi yoluyla sahte bir GPS sinyali oluşturulmaktadır. Şekil 4.2'de uygun girdiler kullanılarak GPS-SDR-SIM kütüphanesi aracılığıyla oluşturulan veri setleri için bir kullanım örneği verilmiştir. Bu, laboratuvar ortamlarında kontrol edilebilir ve tekrarlanabilir bir deney yapılmasına imkan tanırken, aynı zamanda GPS sinyali aldatma saldırılarının potansiyelini de değerlendirmek üzere kullanılan bir simülasyon aracı olarak hizmet verir.



Şekil 4.2 GPS-SDR-SIM Veri Oluşturma Ekranı

Bu yöntemle, GPS L1 C/A sinyalleri simüle edilerek veriler oluşturulmuştur. GPS-SDR-SIM kütüphanesi kullanılarak çeşitli senaryolar oluşturulmuş ve bu veriler üzerinden analizler yapılmıştır.

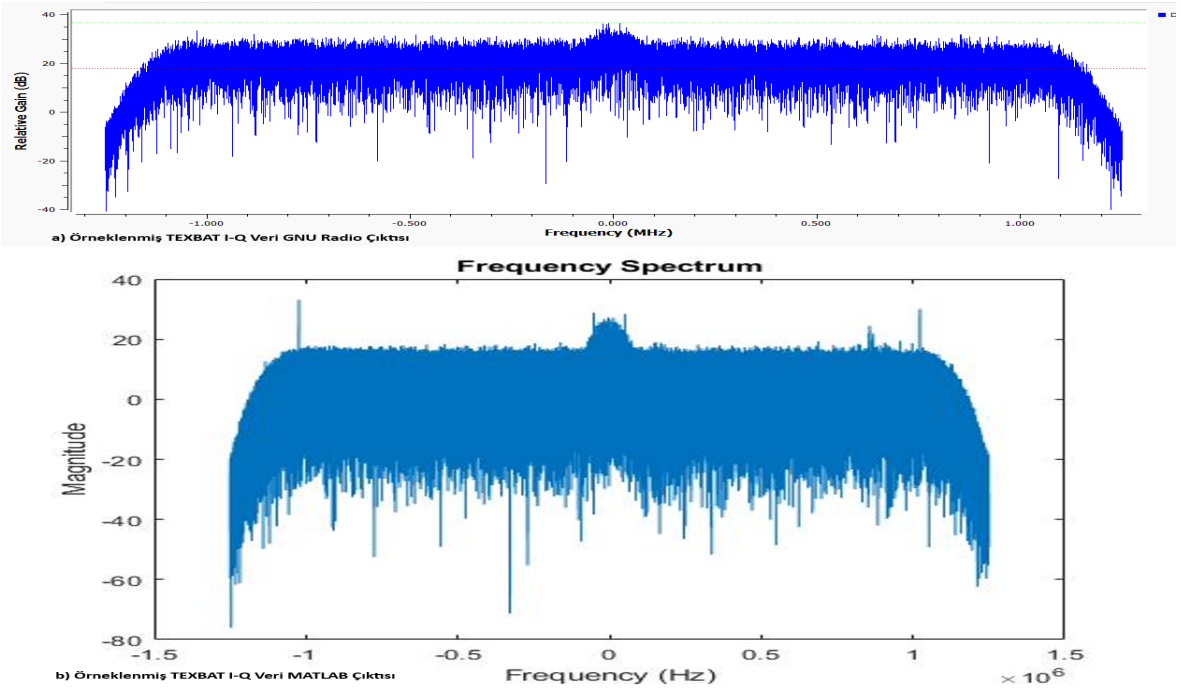
Üretilen sinyalin örneklenmiş bir çıktısı MATLAB ve GNU Radio Programı tarafından alınmış ve karşılaştırılmıştır. Yayının çıktıları Şekil 4.3'te gösterilmiştir ve aralarındaki tutarlılık gözlemlenmiştir.



Şekil 4.3 Örneklenmiş GPS-SDR-SIM I-Q Verileri Çıktışları

4.2.13. TEXBAT kütüphanesi GNSS Verisi İncelenmesi TEXBAT (Texas Spoofing Test Battery), Texas Üniversitesi Radionavigation Laboratuvarı tarafından geliştirilen, sivil GPS sinyal doğrulama tekniklerinin değerlendirilmesi ve geliştirilmesi amacıyla oluşturulmuş altı yüksek kaliteli dijital kayıt setinden oluşmaktadır. Bu veri seti, sivil GPS alıcılarının aldatmaya karşı direncini tanımlayan ve gelişmekte olan bir standardın veri bileşeni olarak kabul edilmektedir. Kayıtlar, GPS sinyal sahteciliği senaryolarını aslına uygun şekilde temsil etmek üzere tasarlanmış olup, hem statik hem de dinamik saldırı koşullarını kapsamaktadır. Kayıt prosedürü, hedef alıcının saf, aldatılmamış koşullardaki tepkilerini gözlemlemeyi ve ardından aynı testleri sadece sahte sinyallerin varlığı ile tekrar etmeyi mümkün kılacak şekilde yapılandırılmıştır. Her bir sahtecilik senaryosu, hedef alıcı üzerinde analiz edilerek, sahte sinyallerin varlığını gösterebilecek belirgin anormallikleri ortaya koymuştur. Sahte ve gerçek sinyallerin karışımı, hedef alıcı tarafından doğal çoklu yol ve solma etkilerinden ayırt edilebilirse, bu etkileşim sahtecilik göstergesi olarak kullanılabilir. Band içi güç izleme ve karmaşık korelasyon fonksiyonu izleme gibi yöntemler, özellikle statik alıcılarda, aldatıcının sinyal gücü avantajını ortadan kaldırma kabiliyetini sınırlayarak sahteciliğin tespit edilmesini sağlar.

TEXBAT kütüphanesinden alınmış bir test sinyalinin çıktısı MATLAB ve GNU Radio Programı tarafından alınmış ve karşılaştırılmıştır. Yayının çıktıları Şekil 4.4'te gösterilmiştir ve aralarındaki tutarlılık gözlemlenmiştir.



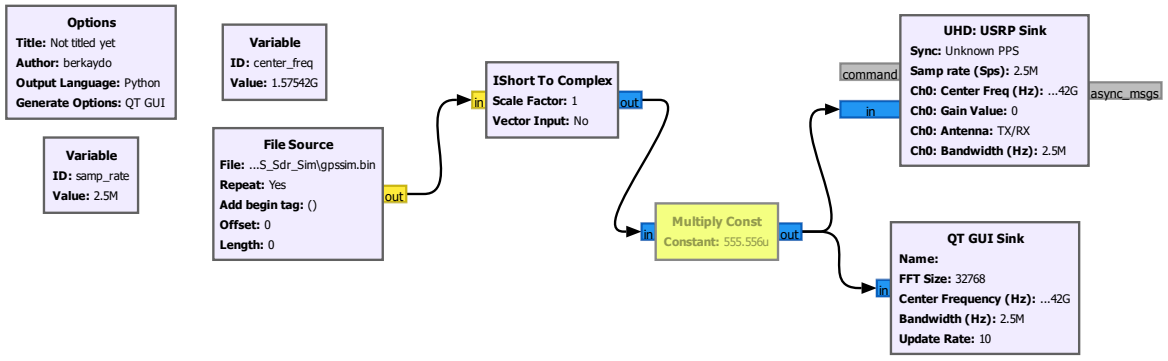
Şekil 4.4 Örneklenmiş TEXBAT I-Q Verileri Çıktıları

4.2.2 Toplanan Verilerin USRP ile Yayınlanması

Toplanan GNSS verileri, USRP cihazı kullanılarak yayınlanmıştır. Bu süreçte, verilerin doğru bir şekilde yayınlanması ve sinyal bütünlüğünün korunması önemlidir. Farklı yöntemlerle elde edilen I-Q verileri, USRP'nin vericisi tarafından GNU Radio yazılımından faydalanılarak yayınlanmıştır. USRP'nin verici kısmına dipol anten takılmıştır ve USRP, toplanan I-Q verilerini 1575,42 MHz frekansındaki radyo frekansı sinyaline çevirmektedir.

Navigasyon sinyalinin gücü, CNR $= C/N_0$ formülü ile ifade edilir, burada CNR alıcıdaki taşıyıcı-gürültü oranını (carrier-noise-ratio), C alıcıdaki taşıyıcı sinyal gücünü (Watt) ve N_0 alıcıdaki gürültü güç yoğunluğunu (Watt/Hz) gösterir. CNR parametresi GPS alıcıları tarafından uydulardan gelen sinyalin kalitesini değerlendirmek için kullanılır. GPS'in L1 bandı sinyali için, alınan sinyal gücünün, gerçek uydulardan gönderilen gerçek taşıyıcı

sinyali gücü ile aynı olduğu varsayılmaktadır. Genel olarak, L1 bandı GPS alıcısının CNR değeri 37 dB ila 45 dB arasındayken, sahtecilik için bu değer 46 dB'ye eşit veya üzerinde olmalıdır. Bu çalışmada sinyal gücü, toplanan sinyalin GNU Radio yazılımı üzerinden sabit katsayı ile çarpılmasıyla kontrol edilecektir. Şekil 4.5'te GNU Radio yazılımı kullanılarak oluşturulan verici modeli gösterilmiştir.

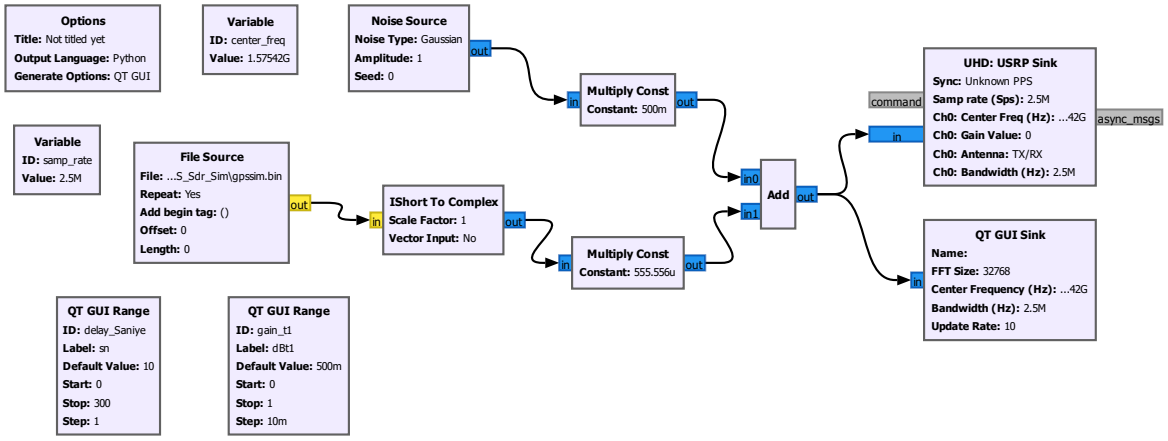


Şekil 4.5 GNU Radio Yazılımı Verici Modeli

Yayınlanan veriler, aldatma ve karşı tedbir yöntemlerinin test edilmesi için kullanılmıştır.

4.2.3 GPS Aldatma Yöntemlerine Gürültü Kaynağı Etkisi

GPS aldatma yaparken GPS L1 frekansında yayın yapan bir gürültü kaynağı Şekil 4.6'da gösterildiği gibi deneylere dahil edilmiştir.



Şekil 4.6 Gürültü Kaynağı Eklenmiş Aldatma Sistem Modeli

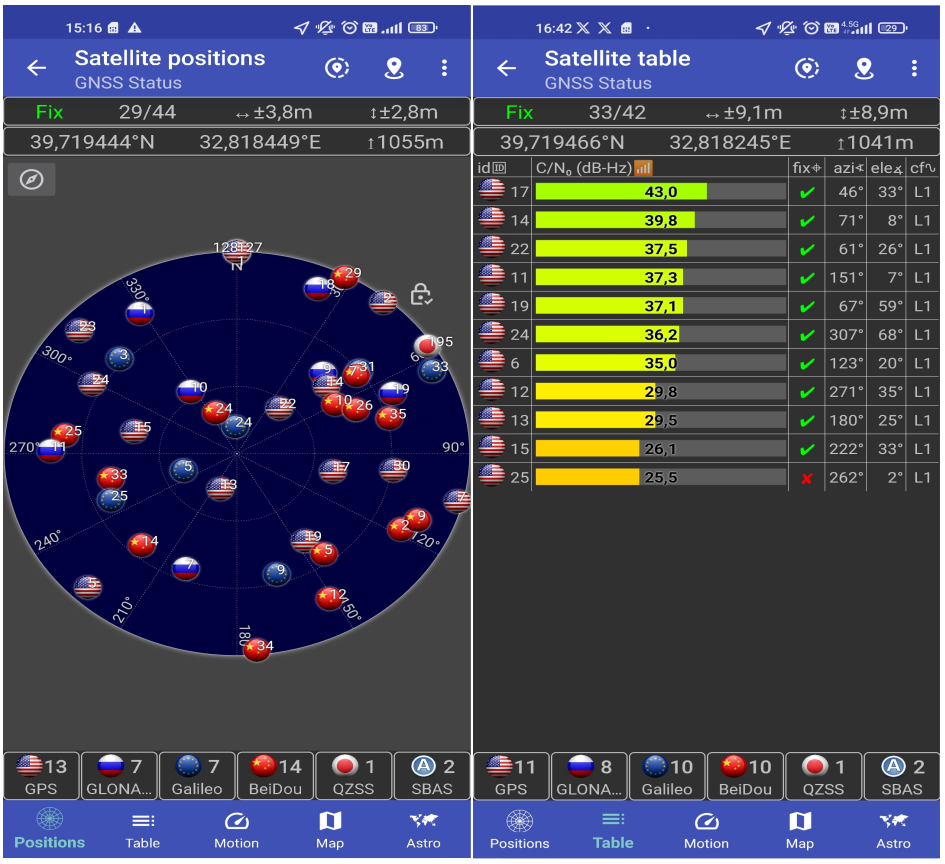
Burada gürültü kaynağının kullanılmasının 2 temel nedeni vardır. Birincisi GPS L1 bandından yüksek güç uygulayarak karıştırma sağlamak ikincisi ise gürültü seviyesini yükselterek CNR kontrolünü sağlayarak kontrollü deney ortamı sağlamak. CNR seviyesinin kontrol edilmesi ile CNR seviyesine bağlı olarak kullanılan karşı tedbir yönteminin de üstesinden gelinmeye çalışılmıştır.

Bu çalışmada gürültü kaynağı eklentisinin özellikle dış ortamlarda yapılan testlerde aldatılma süresine katkıları olduğu gözlemlenmiştir. Dış ortamda gerçek GPS sinyallerine kilitlenmiş alıcıların önce karıştırma sağlanarak karıştırılması ve hemen ardından aldatma sinyalinin yayınlanması ile aldatılma süresinin düştüğü yani aldatılmanın daha kısa sürede yapılabildiği gözlemlenmiştir.

4.2.4 İç Ortam Aldatma Saldırısı Deneyleri

İç ortam deneyleri, GNSS aldatma ve karşı tedbir yöntemlerinin kapalı ve kontrollü bir ortamda test edilmesini amaçlar. Bu deneyler, dış ortam faktörlerinin etkisini en aza indirgemek ve daha kesin sonuçlar elde etmek için yapılır. 39.719447 , 32.8177494 konumununa çok yakın bir konumda iç ortamda yapılan deney sonuçları aşağıdaki şekillerde anlatılmıştır. Deneylerin yapıldığı iç ortamda herhangi bir GNSS verisi bulunmamaktadır.

İç ortamda yapılan ilk deneyde cep telefonu alıcısı yeniden oynatma aldatma saldırısına maruz bırakılmıştır. Önceden toplanan GNSS verileri yayınlanarak cep telefonu ”GNSS Status” uygulaması üzerinden GNSS verileri gözlemlenmiştir. Uygulama üzerinden cep telefonunun gördüğü GNSS uydularının listesini, takımyıldız diyagramını, CNR değerlerini (dB-Hz cinsinden), uyduların sVidlerini, kilitlenilen konum bilgisinin enlem-boylam-yükseklik bilgileri incelenebilmektedir. Cep telefonu bir konum bilgisine kilitlendiğinde uygulama üzerinde yeşil yazı ile ’Fix’ bilgisi gösterilmektedir. Şekil 4.7’de görüldüğü gibi cep telefonunun ortamda GNSS sinyali olmamasına rağmen GNSS sinyallerini gördüğü ve ilgili konum bilgisine kilitlendiği görülmektedir. Cep telefonu yeniden aldatma saldırısı ile iç ortamda başarıyla aldatılmıştır.

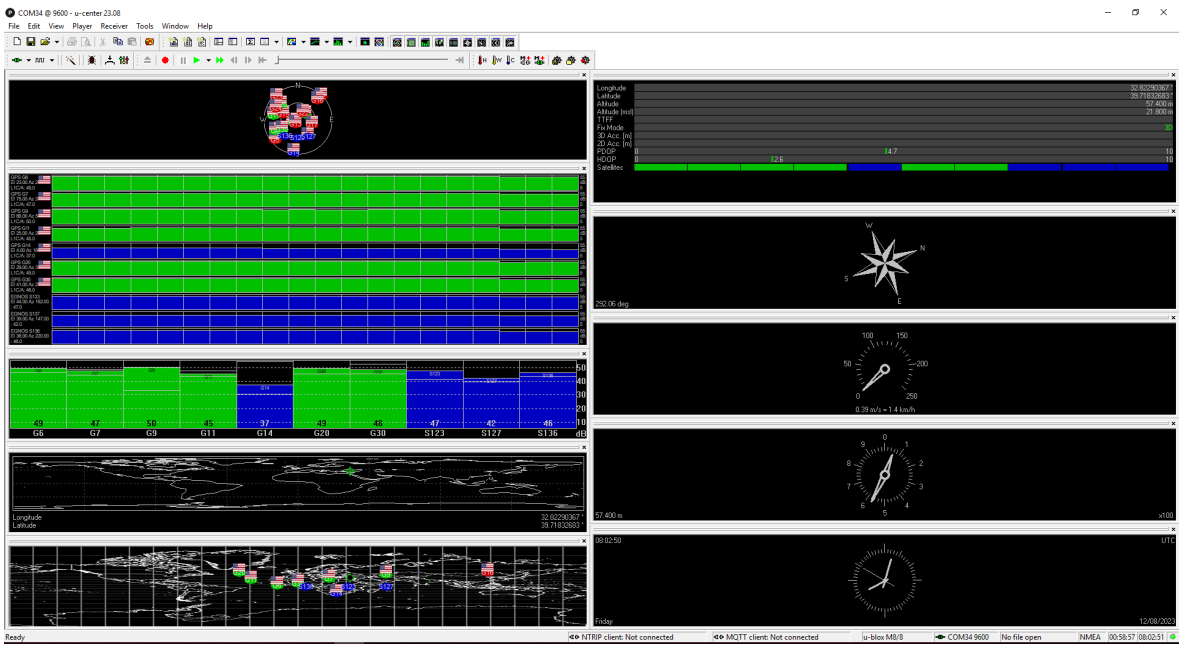


Şekil 4.7 Yeniden Oynatma Aldatma Saldırısı ile İç Ortamda Cep Telefonu Aldatma Deneyi

Farklı modeldeki cep telefonları ile deneyler yapılmıştır. Qualcomm Snapdragon 865, Exynos 990 ve Exynos 1380 platformlarındaki gömülü GNSS alıcılarında aldatma yapılabildiği gözlemlenmiştir. Her bir cep telefonu için aldatılma süreleri not edilmiştir. Aldatılma süreleri cep telefonlarına göre değişkenlik gösterdiği için ortalama değerler hesaplanmıştır.

Yeniden oynatma saldırısının iç ortamda UBLOX M8N alıcısı üzerindeki etkileri de gözlemlenmiştir. UBLOX M8N alıcısındaki GNSS verileri bir seri kanal bağlantısı üzerinden 'ucenter' uygulaması ile incelenmiştir. Uygulama üzerinden cep telefonu uygulamasına benzer şekilde alıcının gördüğü GNSS uydularının listesini, takımyıldız diyagramını, CNR değerlerini (dB-Hz cinsinden), uyduların sVidlerini, kilitlenilen konum bilgisinin enlem-boylam-yükseklik bilgileri, HDOP, PDOP gibi önemli GNSS verileri incelenebilmektedir. Alıcının bir konum bilgisine kilitlendiğinde, verilerini kullandığı

uydularının yeşil renge dönüştüğü ve ekranın sağında bulunan 'Fix Mode' değerinin '3D' olduğu gözlemlenmektedir. Şekil 4.8'de UBLOX M8N alıcısının iç ortamda yeniden aldatma saldırından etkilendiği ve aldatıldığı görülmektedir. Cep telefonlarında olduğu gibi UBLOX M8N alıcısının da aldatılma süresi not edilmiştir ve yapılan deneyler sonucundaki aldatılma süresi bilgisinin ortalaması alınmıştır.



Şekil 4.8 Yeniden Oynatma Aldatma Saldırısı ile İç Ortamda UBLOX Aldatma Deneyi

Sahtecilik aldatma saldırısının etkileri de yine aynı model cep telefonları ve UBLOX alıcısı üzerinde denenmiştir. Şekil 4.9'da Cep telefonunun GPS-SDR-SIM kütüphanesi tarafından üretilmiş veriler ile sahtecilik aldatma saldırısı altındaki tepkisi gözlemlenmiştir. Görüldüğü gibi cep telefonu kendisini 39.719447 , 32.8177494 koordinatlı Ankara konumundayken 35.681274 , 139.766199 koordinatlı Tokyo konumuna kilitlenmiş olarak görmektedir. Cep telefonunun sahtecilik aldatma saldırısı karşısında aldatıldığını ve deneylerin başarılı olduğu gözlemlenmektedir.

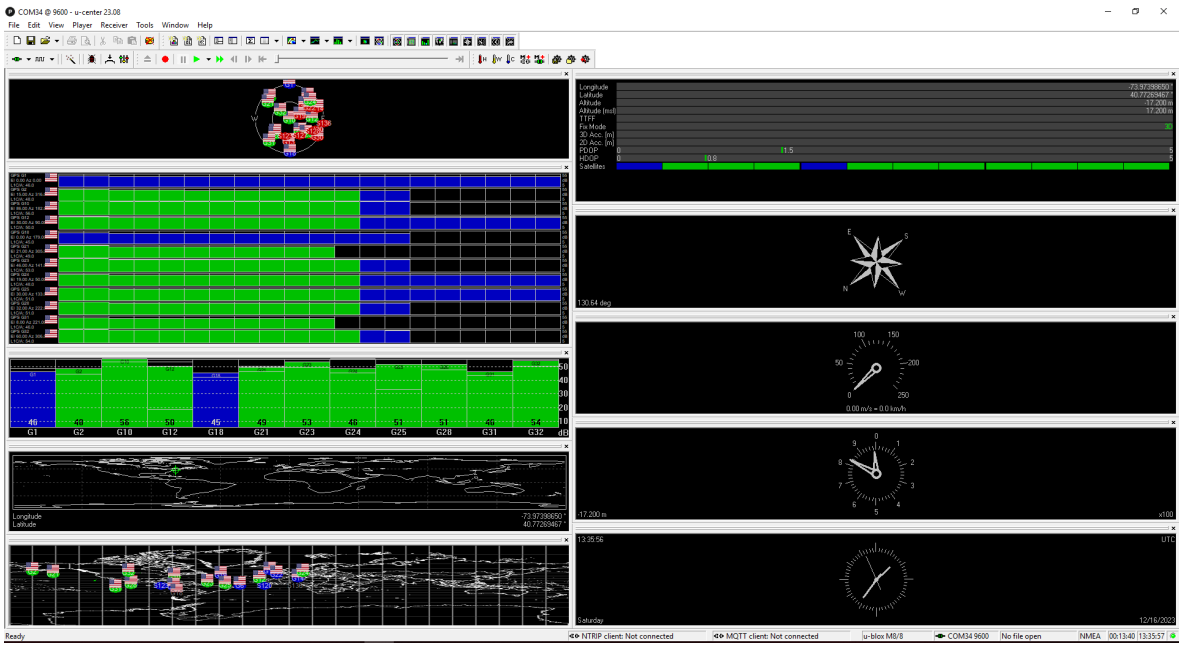
Şu ana kadar anlatılan iç ortamda yaptığımız aldatma saldırıları deneylerinde alıcıların benzer aldatılma sürelerinde aldatıldığı görülmektedir. İç ortamdaki deneylerde yakın mesafe aldatma veya uzak mesafe aldatmanın etkilerini gözlemlemek için cep telefonlarına ve UBLOX alıcısna farklı konum bilgilerine göre aldatma deneyleri yapılmıştır. Şekil 4.10'da

Şekil 4.9 Sahtecilik Aldatma Saldırısı ile İç Ortamda Cep Telefonu Aldatma Deneyi

en son konumu Tokyo olarak gösterilen cep telefonun dünyanın diğer ucundaki New York şehrine gönderilmesi denenmiştir. Bu deney sonucunda iç ortamda aldatılma süresi yaklaşık 30 saniye olan cep telefonu alıcısının uzak mesafe farketmeksizin yine 30 saniye içinde aldatıldığı tespit edilmiştir. Aldatma yapılan konumlar arasındaki mesafenin artmasının iç ortam deneylerinde aldatılma süresine etkisi olmadığı gözlemlenmiştir.

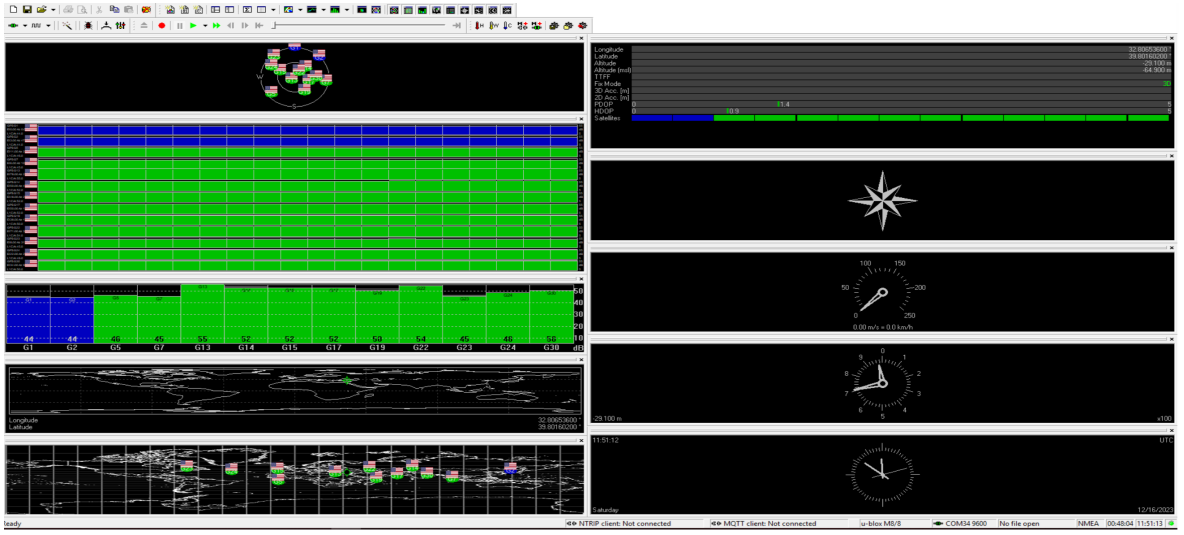
Şekil 4.10 Sahtecilik Aldatma Saldırısı ile İç Ortamda Cep Telefonu Aldatma Deneyi Uzak Mesafe

UBLOX M8N alıcısına uygulanmış sahtecilik saldırılarında da Şekil 4.11'de gösterildiği gibi aldatmanın başarılı olduğu gözlemlenmiştir.



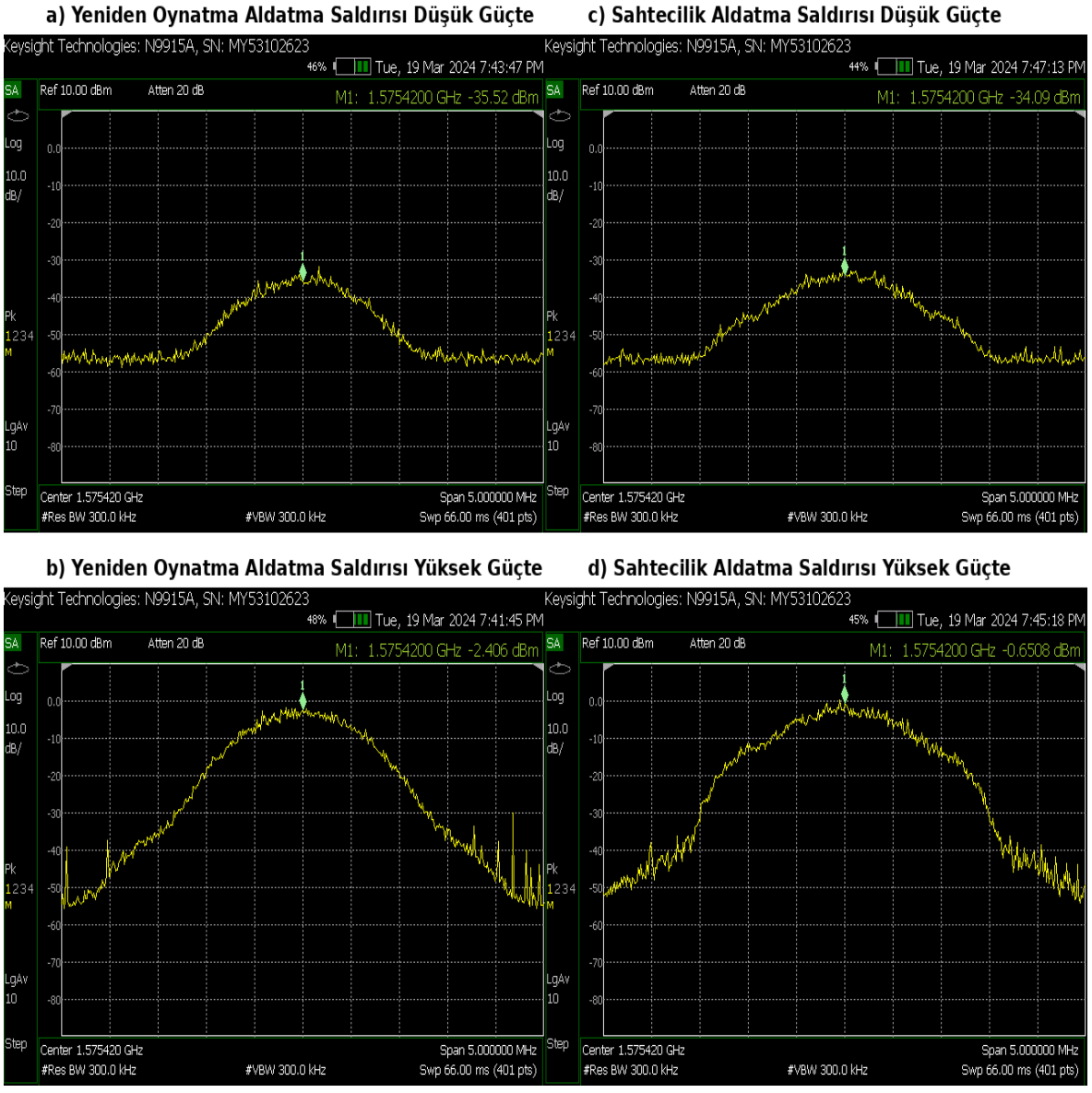
Şekil 4.11 Sahtecilik Aldatma Saldırısı ile İç Ortamda UBLOX Aldatma Deneyi

Yapılan ilk sahtecilik aldatma deneyinde New York şehri konum bilgisine kilitlenmiş olan UBLOX alıcısı hemen ardından yayınlanan gerçek konuma yaklaşık 20 kilometre mesafede bulunan Ankara şehir içi bir konuma göre aldatılma yapılan alıcı yine benzer şekilde yaklaşık 30 saniye içerisinde aldatılmıştır. Şekil 4.12'de gösterildiği gibi UBLOX M8N alıcısı için de birbiri ardına yayınlanan konum sinyalerinin konum bilgilerinden çıkartılan mesafelerin farklı olmasının iç ortamlarda aldatılma süresine etkisi olmadığı gözlemlenmiştir.



Şekil 4.12 Sahtecilik Aldatma Saldırısı ile İç Ortamda UBLOX Aldatma Deneyi Yakın Mesafe

İç ortamda yayınlanan sinyallerin spektrum analizör yardımıyla spektrum verileri alınmıştır. Şekil 4.13'te gösterildiği gibi USRP'nin kazancı 0dB ve 40dB ayarlanmışken yapılan yeniden oynatma ve sahtecilik aldatma saldırıları gösterilmiştir.



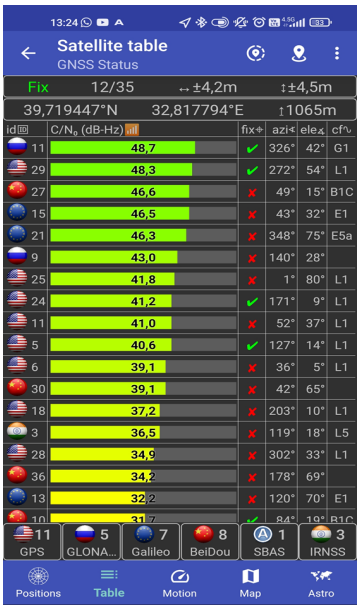
Şekil 4.13 İç Ortamda Aldatma Saldırısı Spektrum Görüntüsü

4.2.5 Dış Ortam Aldatma Saldırısı Deneyleri

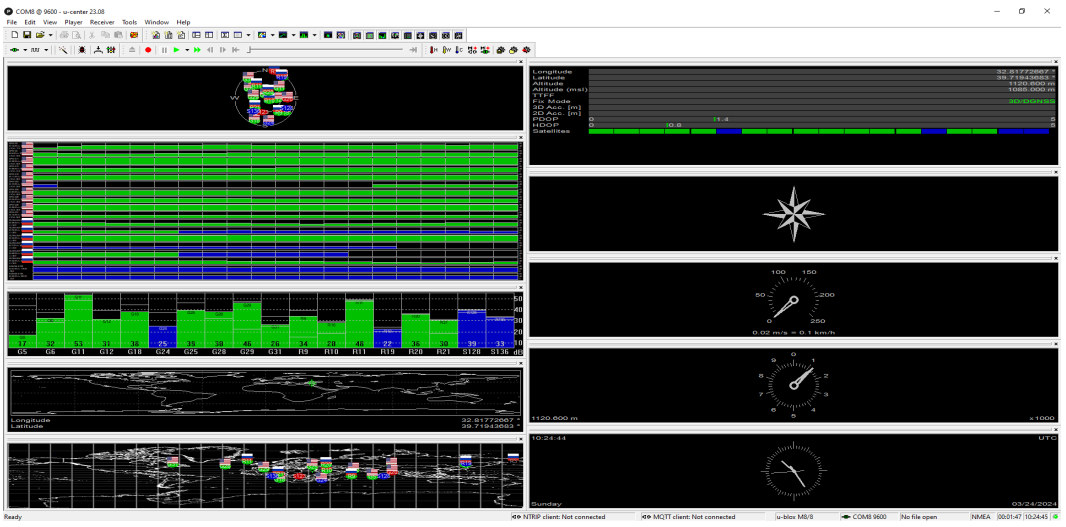
Dış ortam deneyleri, GNSS aldatma ve karşı tedbir yöntemlerinin açık ve kontrolsüz çevre koşullarında test edilmesini amaçlar. Bu deneyler, gerçek dünya senaryolarını yansıtmak ve dış ortam faktörlerinin etkilerini gözlemlemek için önemlidir. Dış ortamda yapılan deneyler 39.719447 , 32.817794 konumunda uygulanmıştır. Deney kurulumu Şekil 4.14'te gösterildiği gibidir. Dış ortamlarda yapılan aldatma deneylerinde test bilgisayarı, USRP, spektrum analizör, bias tee, güç kaynağı ve antenler kullanılmıştır. Deneylerde aldatılmanın başarılı olması ve alıcıların aldatılma süreleri gözlemlenmiştir. Bu deneyler, GNSS aldatma saldırılarına maruz kalan cihazların verdiği tepkileri ve bu tepkilerin doğruluğunu ölçerek, saldırıların gerçek dünya koşullarında nasıl işlediğini anlamamıza yardımcı olacaktır.

Şekil 4.14 Dış Ortam Deney Kurulumu

Dış ortamlarda, gerçek GNSS sinyalleri mevcuttur ve bu sinyaller, kullanılan alıcıların doğru konum bilgisine kilitlenmesini sağlar. Deneylere başlanmadan önce, tüm alıcılar gerçek konum bilgisine kilitlenmiş olup, bu durumun doğruluğu teyit edilmiştir. Şekil 4.15 ve Şekil 4.16'da cep telefonu ve UBLOX alıcısının gerçek konum bilgisine kilitlendiği açıkça gösterilmiştir. Bu deneylerde, GNSS alıcılarının kilitlenmiş olduğu gerçek konum bilgisini karıştırmak veya aldatmak amacıyla çeşitli yöntemler uygulanmıştır. Özellikle, karıştırma etkisi ve yüksek güçlü aldatma saldırısı teknikleri kullanılarak, alıcıların konum doğruluğu üzerinde nasıl etkiler yaratılabileceği incelenmiştir. Deneylerin amacı, bu tür saldırıların gerçek dünya koşullarında GNSS alıcılarını nasıl etkilediğini ve alıcıların bu saldırılara karşı nasıl tepkiler verdiğini değerlendirmektir.

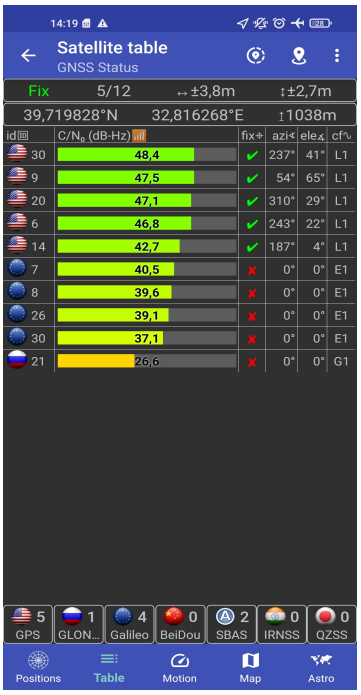


Şekil 4.15 Dış Ortam Deneyleri Cep Telefonu Gerçek Konum Bilgisi



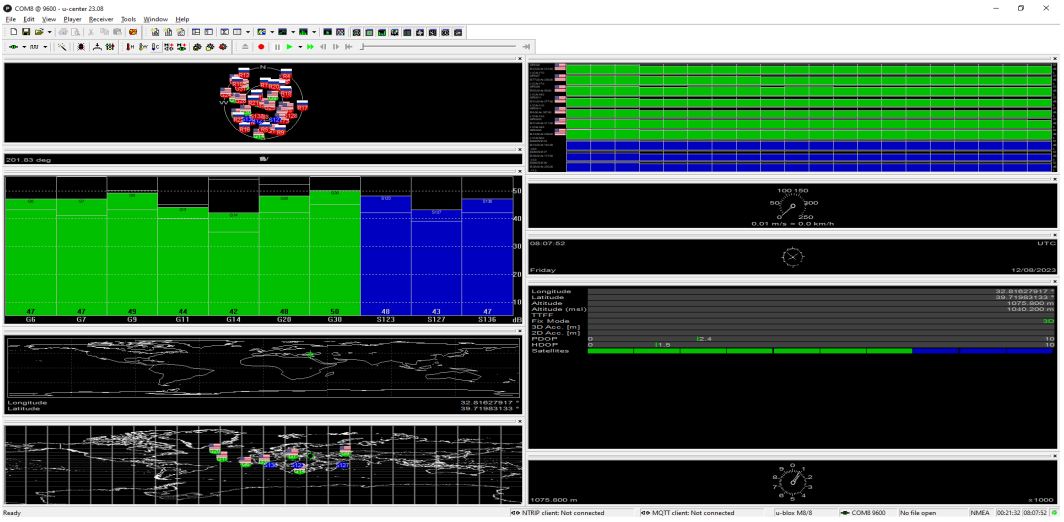
Şekil 4.16 Dış Ortam Deneyleri UBLOX Gerçek Konum Bilgisi

Dış ortamda yapılan yeniden oynatma aldatma saldırısının cep telefonu üzerindeki etkileri Şekil 4.17'de gözlemlenmiştir. Aldatmanın cep telefonu uçak moduna aldığında başarılı olduğu gözlemlenmiştir. Cep telefonlarında A-GNSS özelliği mevcuttur. Cep telefonun dış ortamlarda aldatılabilmesi için güncel efemeris verilerine ihtiyaç vardır çünkü cep telefonları A-GNSS özelliğini kullanarak güncel efemeris verilerini internet üzerinden alarak elde edilen veriler ile karşılaştırmaktadır.



Şekil 4.17 Yeniden Oynatma Aldatma Saldırısı ile Dış Ortamda Cep Telefonu Aldatma Deneyi

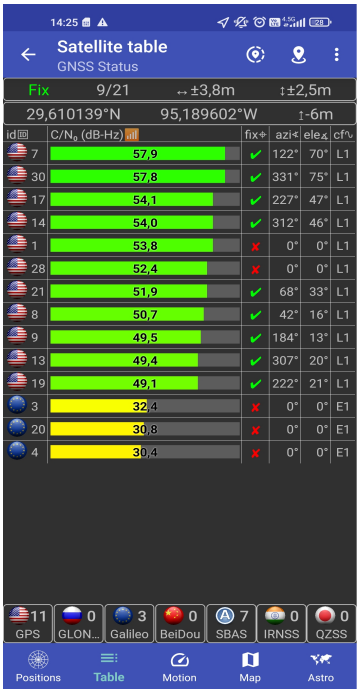
UBLOX M8N alıcının ise herhangi bir karşı tedbir yeteneği olmadığı ve doğrudan aldatılabildiği gözlemlenmiş. UBLOX M8N alıcısının yeniden oynatma aldatma saldırısı altındaki tepkisi Şekil 4.18'de gösterilmektedir.



Şekil 4.18 Yeniden Oynatma Aldatma Saldırısı ile Dış Ortamda UBLOX Aldatma Deneyi

Sahtecilik ile yapılan aldatma saldırısında ise yine UBLOX ve cep telefonunun

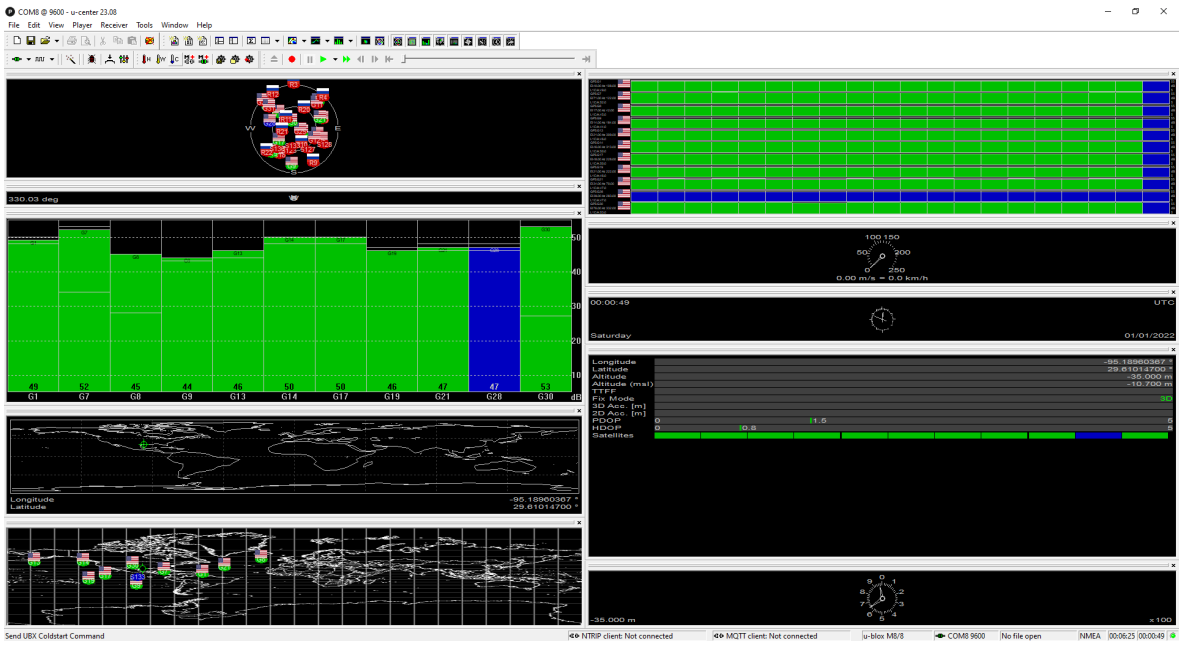
aldatılabildiği gözlemlenmiştir. Rasgele belirlenmiş 29.610139 , 95.189602 konum bilgisinin GPS-SDR-SIM kütüphanesi ile üretilmesi ile aldatma deneyi yapılmıştır. Cep telefonundaki A-GNSS karşı tedbirinden kurtulmak için güncel efemeris verileri kullanarak veriler üretilmiş ve yayınlanmıştır. Şekil 4.19'da görüldüğü gibi güncel efemeris verileri kullanıldığında cep telefonu interneti açık olmasına rağmen aldatılma yapılabildiği görülmektedir.



Şekil 4.19 Sahtecilik Aldatma Saldırısı ile Dış Ortamda Cep Telefonu Aldatma Deneyi

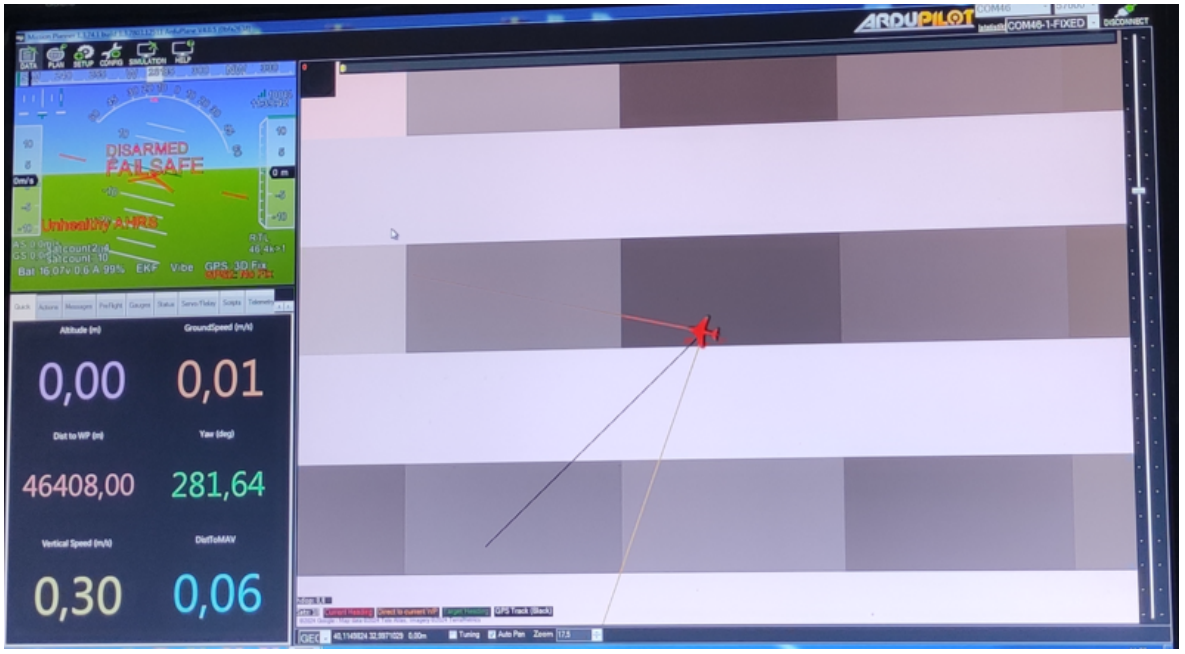
Şekil 4.20'de UBLOX M8N alıcısının aynı sahtecilik aldatma saldırısı altındaki tepkisi gösterilmektedir. Bu deneylerde, sahtecilik aldatma saldırıları sonucunda UBLOX M8N alıcısının da aldatılabildiği ve sahte konum bilgisine kilitlendiği gözlemlenmiştir. Bu durum, aldatma saldırılarının etkili olduğunu ve alıcıların güncel efemeris verileri kullanılarak yapılan sahtecilik saldırılarına karşı savunmasız olduğunu göstermektedir.

GPS aldatma deneyleri UBLOX M8N ve Cep Telefonuna ek olarak 2 adet insansız hava aracı üzerinde bulunan GNSS alıcıları üzerinde de denenmiştir. Şekil 4.21'de dış ortamda bulunan HERE2 GNSS alıcısının sahtecilik aldatma saldırısı altındaki kendi konum takip uygulaması üzerindeki konum görüntüsü görülmektedir. 39.719447 , 32.8177494 konumunda bulunan



Şekil 4.20 Sahtecilik Aldatma Saldırısı ile Dış Ortamda UBLOX Aldatma Deneyi

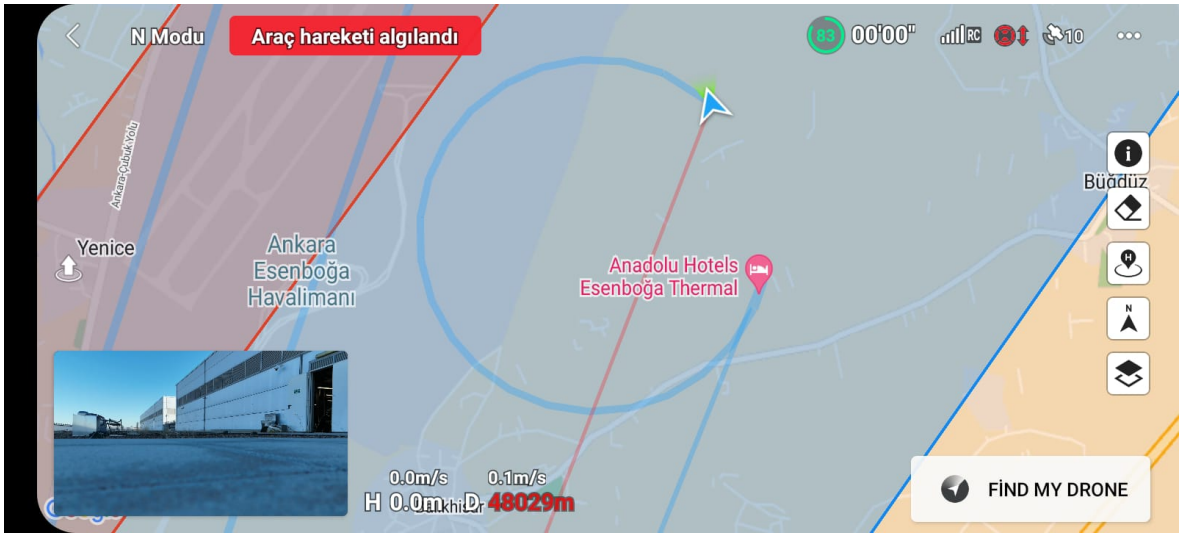
HERE2 GNSS alıcısı kendisini 40.1149824 , 32.9971029 (Ankara Esenboğa Havalimanı) konumunda kilitlenmiş olarak görmektedir.



Şekil 4.21 Sahtecilik Aldatma Saldırısı ile Dış Ortamda HERE2 Aldatma Deneyi

DJI Phantom 4 için yapılan sahtecilik aldatma saldırısı farklı olarak hareketli bir rota

varmışcasına yapılmıştır. GPS-SDR-SIM kütüphanesi kullanılarak üretilen rota bilgisine sahip aldatma yayını altındaki görüntüsü Şekil 4.22'de verilmiştir. HERE2 GNSS alıcısı ile aynı konumda bulunan DJI Phantom 4 IHA'nin 40.11342500993165, 33.01937864968591 konumu başlangıç noktasından itibaren aldatma saldırındaki rotayı izlediği şekilde görülmektedir.

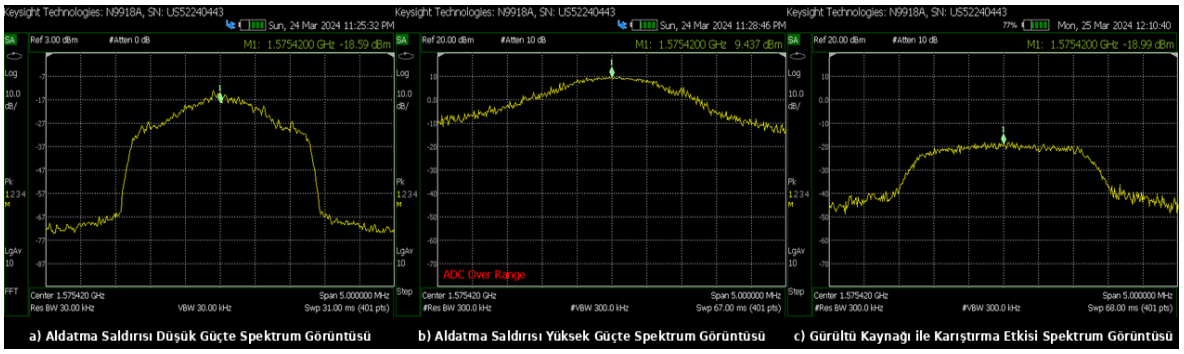


Şekil 4.22 Sahtecilik Aldatma Saldırısı ile Dış Ortamda DJI Phantom 4 Aldatma Deneyi

IHA'larda, cep telefonlarında veya sivil kullınım için üretilen bir çok GNSS alıcısı mevcuttur. Bir çok alıcının bu aldatma saldırısına karşı farklı tepkisi gözlemlenmiştir. Bu çalışmada, yapılan deneyler sonucunda uygulanan sahtecilik aldatma saldırısının kullanılan marka ve modellerdeki IHA'ların ve cep telefonlarının GNSS alıcıları için başarılı performans gösterdiği kanıtlanmıştır. Bütün GNSS alıcıları aynı saldırı altındayken aldatıcıya aynı mesafede konumlandırılmış ve aynı anda gözlemlenmiştir. Deneyler sırasında aldatma saldırılarının başarısız olduğu GNSS alıcılar da mevcuttur. Apple A13 Bionic yonga setine gömülü GNSS alıcısı ve Septentrio AsteRix-m3 alıcısı için aldatma deneyleri başarısız olmuştur.

Bu yapılan deneylerde yeniden oynatma aldatma saldırısı ve sahtecilik aldatma saldırıları farklı stratejilerle de denenmiş ve aldatılma süreleri gözlemlenmiştir. Yeniden oynatma saldırısı yüksek güçlü yeniden oynatma saldırısı ve doğrudan yeniden oynatma saldırısı olarak denenmiştir. Sahtecilik aldatma saldırısı ise doğrudan sahtecilik aldatma saldırısı

ve gürültülü sahtecilik aldatma saldırısı olarak yapılmıştır. Bölüm 4.6'da bahsedilen gürültü kaynağı etkisi gürültülü yeniden oynatma saldırısı olarak gözlemlenmiştir. Şekil 4.23'te kullanılan karıştırma ve aldatma yöntemlerinin spektrum görüntüleri görülmektedir.



Şekil 4.23 Aldatma ve Karıştırma Saldırıları Spektrum Görüntüsü

4.3 GPS Aldatma Saldırılarına Karşı Tedbir Yöntemlerinin Gerçeklenmesi

Bu bölümde, GPS aldatma saldırılarına karşı tedbir yöntemlerinin nasıl gerçeğe dönüştürüldüğü incelenecektir. GNSS alıcılarda CNR (Carrier-to-Noise Ratio), doppler kayması, zaman vb. gibi çeşitli verilerin toplanması ve bu verilerin işlenerek karşı tedbir yöntemlerinin oluşturulması incelenecektir.

4.3.1 GNSS Alıcılarda Verilerin Toplanması

Bu çalışmada, gps aldatma saldırılarına karşı tedbir olabilecek verilerin toplanması Xiaomi Mi 10T model cep telefonunun GNSS alıcısı kullanılarak (Qualcomm Snapdragon 865 yonga setinde entegre GNSS modülü), Android tabanlı 'GNSS Logger' uygulaması ile sağlanmıştır. Veri toplama işlemi hem dış hem de iç ortamlarda gerçekleştirilmiştir ve öncesinde bahsedilen aldatma senaryoları uygulanırken yapılmıştır. GNSS Logger uygulaması, gerçek zamanlı olarak CNR,sVid gibi bir çok veriyi kaydeder ve bu veriler, alıcıların sinyal kalitesini belirlemek ve potansiyel aldatma saldırılarını tespit etmek için kullanılır. Bu verilerinin doğru bir şekilde toplanması ve analiz edilmesi, GNSS sistemlerinin güvenliği

ve güvenilirliği için kritik öneme sahiptir. Bu veriler, aldatma saldırılarının erken tespiti ve önlenmesi için kullanılabilir.

4.3.2 GNSS Alıcılarda CNR ile Aldatma Saldırısı Tespiti

GNSS alıcılarında CNR (Carrier-to-Noise Ratio) verileri, aldatma saldırılarını tespit etmek için etkili bir yöntem olarak kullanılmaktadır. CNR tabanlı tespit yöntemleri kullanılarak sinyal kalitesindeki ani değişimler veya anormallikler belirlenebilmektedir. CNR değerlerinin normal çalışma koşullarında belirlenen referans değerlerle karşılaştırılmasıyla, ani yükselmeler veya beklenmeyen değişiklikler aldatma saldırısı belirtisi olarak değerlendirilmiştir. Bu çalışmada, Sahtecilik Aldatma saldırıları ve CNR değeri doğal sinyallere yakın olacak şekilde kontrol edilerek yapılan aldatma saldırıları incelenmiştir.

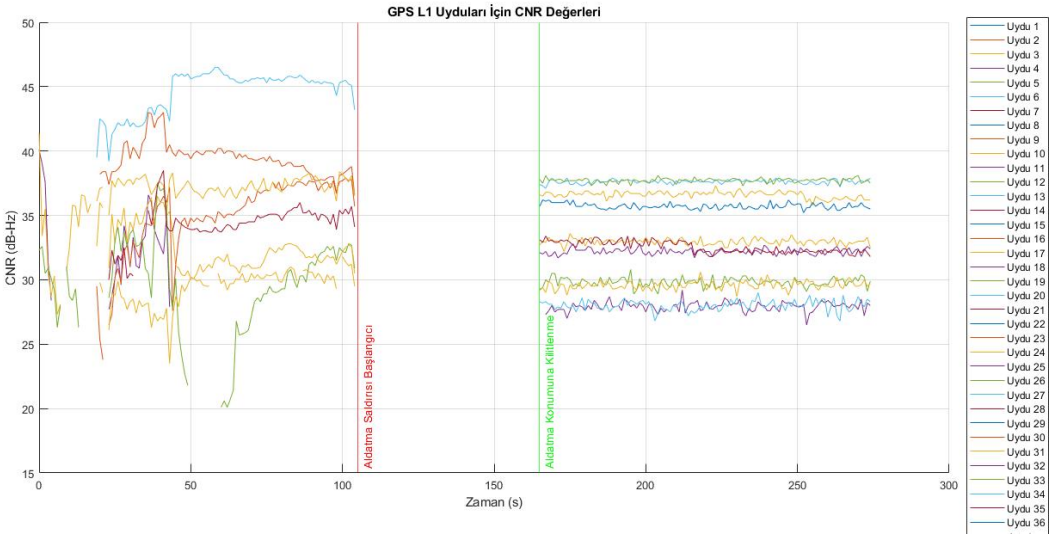
Şekil 4.24'te, zaman ekseninde CNR değerlerinin değişimi gözlemlenmektedir. Grafik incelendiğinde, aldatma saldırısı başlayana kadar olan süreçte gözlemlenen doğal uydulardan yayınlanan CNR değerleri birbirinden oldukca farklılık göstermekte ve CNR değerlerinden 10dB-Hz'e kadar çıkabilen dalgalanmalar görülmüştür. Aldatma saldırısının başladığı (kırmızı çizgi ile belirtilmiş) ve GNSS alıcısının sahte sinyaller tarafından yanıltıldığı andan itibaren GNSS alıcısında karışmalar olduğu ve değerlerin ani değişiklikliklere ve hatta anlamlandıralamamaya başladığı gözlemlenmektedir. Yaklaşık 30 saniye sonra GNSS alıcısının artık sahte uydulardan gelen sinyallere kilitlendiği ve onlardan gelen verileri kullandığı gözlemlenmektedir (yeşil çizgi ile belirtilmiş). Aldatma saldırısının tamamlanmasından sonraki süreçte okunana CNR değerlerinde ani bir yükseliş görülmektedir ve dalgalanmanın doğal sinyallere göre çok daha az olduğu görülmektedir. Doğal uydulardan alınan sinyallerin CNR değerlerinin 20-40 dB-Hz arasında olduğu görülürken aldatma sonrası sahte uydulardan yayınlanan sinyaller için alıcının CNR değerlerini 50-60 dB-Hz olarak aldığı görülmektedir. Bu gözlemler aldatma sinyallerini tespit için kritik ipuçlarıdır.

Sahtecilik aldatma saldırısı altında yapılan gözlemler sonuunda CNR ile aldatma tespitini zorlaştırmak için yeni bir aldatma yöntemi denenmiştir. Bu yöntemde kullanılan GPS sinyali

Şekil 4.24 Aldatma Saldırısı Altında CNR Zaman Grafiği

yayınlanmadan önce GPS L1 frekansında bir gürültü ile toplanılarak yayınlanmıştır. Bu sayede CNR kontrol edilerek aldatma saldırısı yapılmıştır. Şekil 4.25'te CNR değeri doğal sinyallere yakın olacak şekilde kontrol edilerek yapılan aldatma saldırısı altında zamana karşı CNR değerleri grafiği gösterilmiştir. Aldatma saldırısı öncesinde (kırmızı çizgi ile gösterilmiş) tekrardan doğal GPS sinyalleri gözlemlenmiştir. Önceki deneyde olduğu gibi doğal uydulardan yayınlanan sinyallerin CNR değerleri 20-40 dB-Hz arasında dalgalanmakta ve yaklaşık 10 dB-Hz civarında sapmalar göstermektedir. Aldatma saldırısı başladığında gürültü yayının da etkisiyle alıcının yaklaşık 60 saniye boyunca kilitlenemediği ve CNR verisinin alınamadığı gözlemlenmiştir. Aldatma saldırısının başarılı olmasından sonra ise CNR değerleri daha stabil ve doğal sinyal seviyelerine yakın görünmektedir. Ancak, yine de doğal sinyallerin olduğu zaman aralıklarında küçük dalgalanmalar ve anomaliler tespit edilebilirken aldatma saldırısı altında daha sabit CNR değerleri gözlemlenmiştir.

Bu tür küçük değişiklikler, daha sofistike bir aldatma saldırısının belirtisi olabilir. Aldatma saldırısı başladığında (kırmızı çizgi ile belirtilmiş) ve aldatma konumuna kilitlendiğinde (yeşil çizgi ile belirtilmiş), CNR değerlerinde gözle görülür değişiklikler olmuştur. Bu değişiklikler, sahte sinyallerin doğal sinyallere benzer CNR seviyelerinde iletildiğini göstermektedir.



Şekil 4.25 CNR Kontrollü Aldatma Saldırısı Altında CNR Zaman Grafiği

Aldatma saldırılarını tespit etmek için CNR değerlerindeki ani değişikliklerin izlenmesi gerekmektedir. Bu değişiklikler, sinyal kalitesinde ani düşüşler veya anormal dalgalanmalar şeklinde olabilir. Bu tür anomalileri tespit etmek için bir eşik değeri (threshold) belirlemek kritik öneme sahiptir. Eşik değeri, normal çalışma koşullarında CNR değerlerinin ortalaması ve standart sapmasına göre belirlenebilir. Anomaliler, CNR değerlerinin bu eşik değeri aşması durumunda tespit edilebilir. Bu sayede, aldatma saldırıları erken aşamada tespit edilerek gerekli önlemler alınabilir. CNR kontrollü aldatma saldırısı ile CNR ile aldatma tespitinden sakınılabileceği görülmektedir fakat buna karşılık sonraki başlıklarda verilen aldatma tespiti yöntemleri aldatma tespiti için etkili olacaktır.

4.3.3 GNSS Alıcılarda Uzay Aracı Kimlik Kodu (sVid) Kontrolü ile Aldatma Saldırısı Tespiti

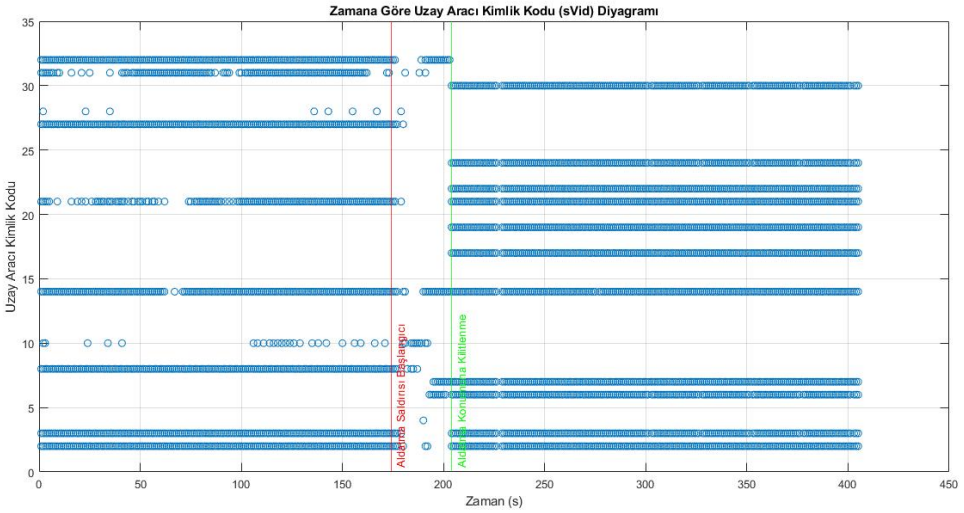
GNSS alıcılarında uzay aracı kimlik kodu (sVid) verileri, aldatma saldırılarını tespit etmek için önemli bir metrik olarak kullanılmaktadır. sVid, GNSS alıcısının algıladığı her bir uydunun kimlik kodunu temsil eder. Bu çalışmada, Sahtecilik Aldatma saldırıları ve CNR değeri doğal sinyallere yakın olacak şekilde kontrol edilerek yapılan aldatma saldırıları incelenmiştir.

GPS yayını yapan uydular dünya etrafında belli orbitaller içerisinde günde 2 tur atmaktadır. Bu sebeple GNSS alıcısının konum bilgisine kilitlendiğinde kullandığı bilgilerin hangi uydulardan sağlandığı sürekli olarak değişmektedir. Buna karşılık kısa süreli bir zaman diliminde sabit konumda alınan GPS sinyalleri aynı uydu gruplarından gelmektedir ve sVid değerlerinde az değişim göstermektedir. Şekil 4.26'da, sabit bir konumda sürekli olarak toplanan veri setinde zaman ekseninde sVid değerlerinin değişimi gözlemlenmektedir. Grafik incelendiğinde, aldatma saldırısı (kırmızı çizgi ile belirtilmiş) başlamadan önce alınan doğal GPS sinyalleri için görüldüğü gibi konum tespiti için kullanılan uydu grubunda çok az değişim olduğu gözlemlenmektedir.

Aldatma saldırısı başladığında verilerin geldiği uydu grubunun sVid değerlerinde karıştırma ve aldatılma etkisiyle dalgalanma başlamıştır. Aldatma saldırsının başarıya ulaşmasından ve alıcının yeniden konum bilgisine kilitlenmesinden (yeşil çizgi ile belirtilmiş) sonra sVid değerlerinde doğal sinyallerden alınan değerlere göre ani değişiklikler meydana gelmiştir. Bu değişiklikler, sahte uyduların GNSS alıcısı tarafından algılandığını ve gerçek sinyaller olarak kabul edildiğini göstermektedir. Bu tür değişiklikler, aldatma saldırılarının tespiti için kritik ipuçlarıdır. Deneyde görüldüğü gibi doğal sinyallerin kullanıldığı sVid değerleri 2,3,8,14,21,27,31,32 uydu gurubundan aldatma sonrasında 2,3,6,7,14,17,19,21,22,24,30 sVid değerlerinde sahip uydu grubuna geçiş olmuştur. Bu ani değişimi gözlemleyerek alıcının aldığı konum bilgilerinden en az 5 veya daha fazla uydunun sVid değerinin anlık değişimi ile aldatma tespiti bu deney için yapılabilmektedir.

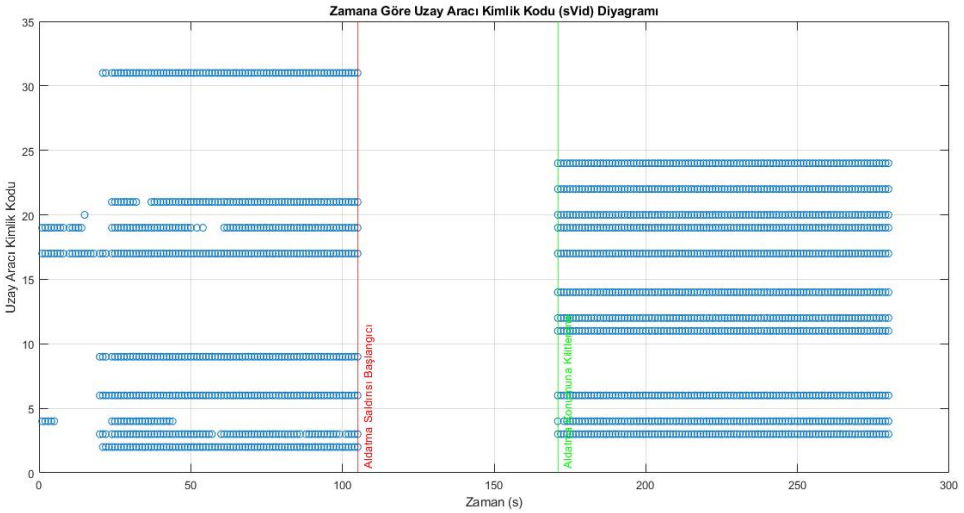
CNR değeri doğal sinyallere yakın olacak şekilde kontrol edilerek yapılan aldatma saldırısında, aldatma saldırısı başlangıcıyla birlikte oluşan karıştırma etkisiyle herhangi bir uydu sVid bilgisi alınamadığı Şekil 4.27'de görülmektedir.

Aldatma saldırısı tamamlanıp alıcının sahte konum bilgisine kilitlenmesi ile gelen uydu bilgilerinde doğal gps sinyallerinden gelen bilgilere göre ani değişimler olmuştur. Önceki deneye benzer şekilde alıcının kullandığı uyduların sVid değerleri 2,3,6,9,17,19,21,31 iken birden 3,4,6,11,12,14,17,19,20,22,24 değerlerine dönüşmüştür. Bu gözlem aldatma saldırısı tespiti yapmak için kullanabilir.



Şekil 4.26 Aldatma Saldırısı Altında sVid Zaman Grafiği

Uyduların hareketli olmasından kaynaklı olarak sabit konumda yeterince beklenildiğinde konum bilgisine ulaşmak için kullanılan uydular değişim gösterebilmektedir. Burada kurguladığımız 2 deney için de aldatma saldırısı sonrasında gelen sVid değerleri için hiç bir değişimin olmaması da aldatma tespiti için bir gözlem olabilmektedir. Çünkü sahte yayınlanan sinyaller için tanımlanan uydu grubu bu deney için sabittir.



Şekil 4.27 CNR Kontrollü Aldatma Saldırısı Altında sVid Zaman Grafiği

GNSS alıcıları, belirli bir konumda belirli zaman aralıklarında belirli uydulardan sinyal

alır. Bu uyduların kimlik kodları (sVid), alıcının konumuna ve zamanına göre tahmin edilebilir. Eğer alıcı, beklenen sVid değerlerinden sapmalar tespit ederse, bu durum aldatma saldırısının belirtisi olabilir. Uyduların konumları ve hareketleri belirli algoritmalar ve modeller kullanılarak tahmin edilebilir. Bu modeller, GNSS alıcılarının belirli zaman dilimlerinde hangi uydulardan sinyal alması gerektiğini belirleyerek, aldatma saldırılarını tespit etmede kullanılabilir. Anormal sVid değerleri tespit edildiğinde, bir alarm sistemi devreye girerek kullanıcıyı uyarabilir ve gerekli önlemler alınabilir.

4.3.4 GNSS Alıcılarda Doppler Kayması ile Aldatma Saldırısı Tespiti

Doppler kayması, GNSS alıcılarında aldatma saldırılarını tespit etmek için kullanılan bir yöntemdir ve uydulardan gelen sinyallerin frekansındaki değişiklikleri analiz ederek anormallikleri belirler. Bu çalışmada, GNSS alıcısı uydulardan gelen sinyallerin Doppler kayma verilerini toplar ve bu veriler, alıcının hareketine ve uyduların konumuna göre beklenen Doppler kayma değerleriyle karşılaştırılarak analiz edilir. Doppler kayma verilerindeki anormal değişiklikler veya beklenmeyen sapmalar aldatma saldırısı belirtisi olarak değerlendirilir ve bir alarm sistemi devreye girerek kullanıcıyı uyarır. Bu yöntem, aldatma saldırılarının erken tespiti ve önlenmesi için etkili bir yol sağlar.

GNSS alıcılarında Doppler kayması verileri, aldatma saldırılarını tespit etmek için etkili bir yöntem olarak kullanılabilir. Doppler kayması, uydu sinyalinin frekansındaki değişim olarak tanımlanır ve uydu ile alıcı arasındaki göreli hızdan kaynaklanır. Bu çalışmada, Sahtecilik Aldatma saldırıları ve CNR değeri doğal sinyallere yakın olacak şekilde kontrol edilerek yapılan aldatma saldırıları incelenmiştir.

Doppler kayması, aşağıdaki formül kullanılarak hesaplanır:

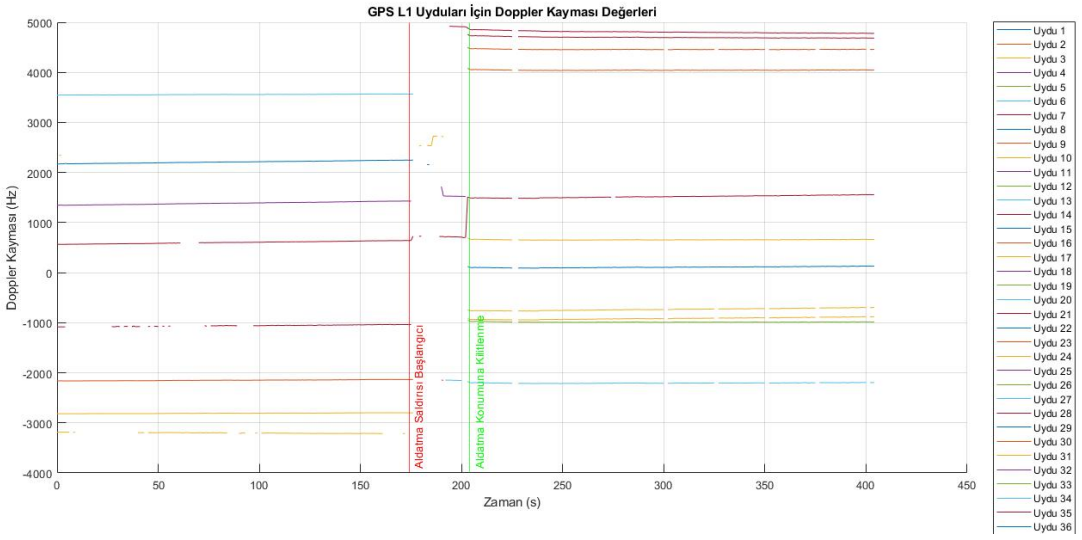
$$\text{Doppler kayması} = \frac{v}{c} \times f_c$$

Burada:

- v: Uydu ile alıcı arasındaki göreli hız (PseudorangeRateMetersPerSecond)
- c: Işık hızı ($\approx 3 \times 10^8$ m/s)
- f_c: Uydu taşıyıcı frekansı (CarrierFrequencyHz)

Şekil 4.28'de, zaman ekseninde Doppler kayması değerlerinin değişimi gözlemlenmektedir. Grafik incelendiğinde, belirli zaman aralıklarında Doppler kayması değerlerinde ani değişiklikler olduğu görülmektedir. Bu değişiklikler, aldatma saldırısının başladığı ve GNSS alıcısının sahte sinyaller tarafından yanıltıldığı anları temsil eder.

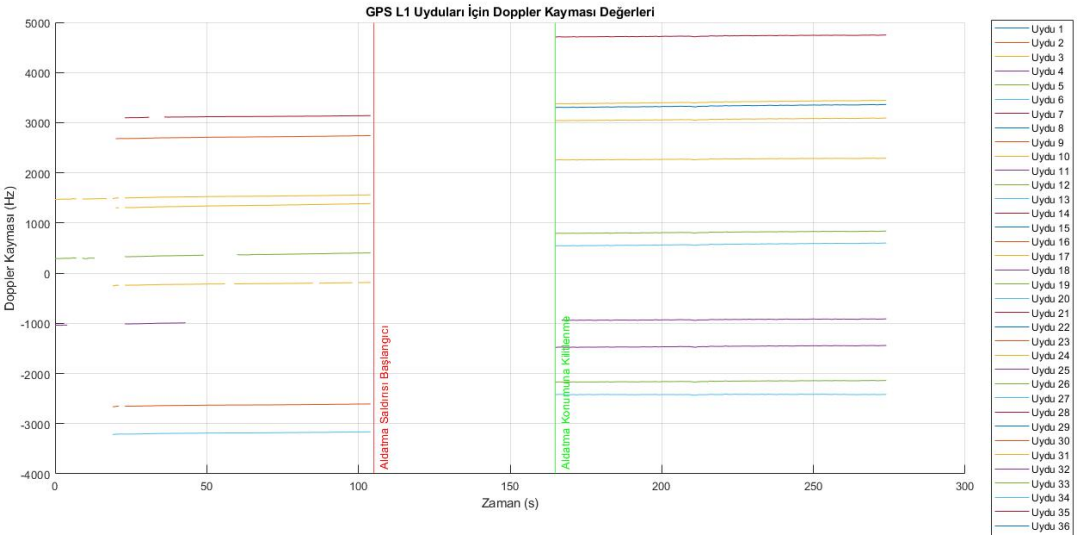
Aldatma saldırısı başladığında (kırmızı çizgi ile belirtilmiş), Doppler kayması değerlerinde keskin değişiklikler meydana gelmiştir. Bu değişiklikler, sahte sinyallerin gerçek sinyalleri bastırdığı ve GNSS alıcısının aldatıldığı anlamına gelir. Bu tür değişiklikler, aldatma saldırılarının tespiti için kritik ipuçlarıdır.



Şekil 4.28 Aldatma Saldırısı Altında Doppler Zaman Grafiği

CNR değeri doğal sinyallere yakın olacak şekilde kontrol edilerek yapılan aldatma saldırısında, Şekil 4.29'da görüldüğü gibi benzer şekilde Doppler kayması değerleri aldatma saldırısının başlamasıyla karışma etkisiyle gözlemlenememiştir. Aldatma saldırısının başarılı olması sonrasında Doppler değerlerinde ani değişiklikler yine gözlemlenmiştir. Zamanla yaklaşık Hz mertebesin değişiklik gösteren Doppler kayması aldatma sonrasında anlık olarak

kHz mertebesinde değişiklik göstermiştir. Yapılan sahtecilik aldatma saldırılarında Doppler etkisinin hesaba katılması bu yöntemin aldatma tespiti için kullanılmasını zorlaştırmaktadır. Fakat yine de ani değişimlerin olması aldatma tespiti için bir ipucu olabilir. Yüksek çözünürlüklü bir alıcı ile Doppler frekansındaki anormallikler daha iyi tespit edilebilir.



Şekil 4.29 CNR Kontrollü Aldatma Saldırısı Altında Doppler Zaman Grafiği

Aldatma saldırılarını tespit etmek için Doppler kayması değerlerindeki ani değişikliklerin izlenmesi gerekmektedir. Bu değişiklikler, sinyal frekansında ani sapmalar veya anormal dalgalanmalar şeklinde olabilir. Doppler kaymasındaki anormallikler, sahte sinyallerin varlığını işaret eder ve bu verilerin sürekli izlenmesi, GNSS alıcılarının güvenliğini artırmak için kritik öneme sahiptir.

Bu sayede, aldatma saldırıları erken aşamada tespit edilerek gerekli önlemler alınabilir. Doppler kayması verileri, GNSS alıcılarında aldatma saldırılarını tespit etmek için etkili bir metrik olup, aldatma saldırılarını algılamak ve önlemek için kullanılabilir.

5 BENZETİMLER ve ANALİZLER

Bu bölümde, bölüm 4.2 ve 4.3'de gerçeğe dönüştürülmüş GPS aldatma ve karşı tedbir yöntemlerinin performansları karşılaştırılacaktır. Deneyler ve analizler sonucunda elde edilen veriler üzerinden bu yöntemlerin etkinlikleri değerlendirilecektir

5.1 GPS Aldatma Yöntemleri Performans Analizi

GPS aldatma deneyleri gerçekleştirilmiş ve bu deneylerin sonuçları analiz edilmiştir. Bu çalışmada, etkinliğinden çok uygulanabilirliğiyle ön plana çıkan yeniden oynatma aldatma saldırısı ve sahtecilik aldatma saldırısı yöntemlerinin farklı stratejilerle kurgulandığı senaryolar denenmiştir.

Yapılan deneylerde elde edilen aldatılma süresi değerleri Tablo 5.1'de verilmiştir. Farklı stratejilerle yapılmış aldatma saldırılarında gürültü etkisinin ve yükseltilmiş gücün aldatılma sürelerine olan etkisi açıkça görülmektedir.

Tablo 5.1 GPS Aldatma Deneyleri Aldatılma Süresi Sonuçları

Aldatma Yöntemleri	**Ortalama Aldatılma Süresi (saniye)**							
	Yeniden Oynatma (Y.O)		Yüksek Güçlü Y.O		Sahtecilik		Sahtecilik ve Gürültü	
	İç	Dış	İç	Dış	İç	Dış	İç	Dış
Exynos 1380 Yonga Seti	29,83	119,95	25,98	50,34	32,82	145,08	26,98	42,52
Exynos 990 Yonga Seti	29,83	119,95	25,98	50,34	32,82	145,08	26,98	42,52
Qualcomm Snapdragon 865 Yonga Seti	29,83	119,95	25,98	50,34	32,82	145,08	26,98	42,52
Apple A13 Bionic	X	X	X	X	X	X	X	X
UBLOX M8N	30	32,89	28,08	30,67	32,76	33,84	25,34	26,78
Here 2	35,21	X	29,54	55,72	30,12	38,55	28,75	34,62
DJI Phantom 4	37,28	X	28,08	172,25	31,20	185,25	30,00	45,24
Septentrio AsteRx-m3	X	X	X	X	X	X	X	X

Alıcıların aldatma saldırısı geçtikten sonra doğal sinyaller altında kaç saniye içerisinde yeniden konum bilgisine kilitlendikleri ve kendilerini toparladıkları süre aşağıdaki tablo 5.2'de verilmiştir. Yapılan deneylerde aldatma sinyali kapatıldıktan sonra alıcıların yeniden toplanma sürelerinin ortalama değerleri alınmıştır fakat aldatma saldırısı sonrasında kendini

toparlayamayan deneyler de olmuştur. Sonuçlar değerlendirilirken ortalama zaman kendini toparlamayı başarabilen değerler için alınmıştır.

Tablo 5.2 GNSS Alıcıların Yeniden Doğal Konuma Kilitlenme Süresi

GNSS Alıcısı	**Yeniden Kilitlenme Zamanı (s)**
Qualcomm Snapdragon 865 Yonga Seti	45,54
Exynos 990 Yonga Seti	45,54
Exynos 1380 Yonga Seti	45,54
UBLOX M8N	85,80
Here 2	91,95
DJI Phantom 4	72,89

Yapılan deneylerde 1W'lık güç ile GNSS alıcılarının yaklaşık 600 metre mesafeden aldatılabildiği gözlemlenmiştir.

5.2 Gerçeklenmiş GPS Aldatma ve Karşı Tedbir Yöntemlerinin Karşılaştırılması

Bu bölümde, gerçekleştirilen GPS aldatma teknikleri ve bu saldırılara karşı geliştirilen tedbir yöntemlerinin performansları karşılaştırılacaktır. Bu amaçla, yapılan deneylerde uygulanan senaryolardaki aldatma yöntemleri ve karşı tedbirler, maliyet, uygulanabilirlik ve performans kriterleri açısından değerlendirilmiştir.

Aldatma yöntemlerinde maliyet, aldatmanın gerçekleştirilmesi için gerekli minimum donanımın maddi karşılığı olarak ele alınmıştır. Uygulanabilirlik, kullanılan aldatma yönteminin hazırlık aşamasında ortaya çıkan işlem yükü doğrultusunda değerlendirilmiştir. Bu işlem yükü; veri toplama, manipülasyon verilerinin eklenmesi ve verilerin yayına hazır hale getirilmesi gibi adımları içermektedir. Performans ise yapılan deneylerde alıcıların aldatılma süreleri, başarılı aldatma oranı ve aldatılabilen alıcı modelleri çeşitliliğinde değerlendirilmiştir.

Tablo 5.3'te sunulan verilere göre, yeniden oynatma saldırısının maliyeti, kaydedilen sinyallerin gerçek zamanlı olarak yeniden oynatılmasının gerektirdiği yüksek bellek kapasitesi nedeniyle orta seviyede değerlendirilmiştir. Bu saldırının uygulanabilirliği, yüksek

Aldatma Yöntemi	Maliyet	Uygulanabilirlik	Performans
Yeniden Oynatma Saldırısı	Orta	Düşük	Orta
Yüksek Güçlü Yeniden Oynatma Saldırısı	Yüksek	Düşük	Yüksek
Sahtecilik Aldatma Saldırısı	Düşük	Yüksek	Orta
CNR Kontrollü Sahtecilik Aldatma Saldırısı	Orta	Düşük	Orta
Karıştırma Sonrası Aldatma Saldırısı	Çok Yüksek	Orta	Yüksek

Tablo 5.3 Gerçeklenmiş Aldatma Yöntemlerinin Değerlendirilmesi

maliyetler ve gerçek zamanlı kayıt alıp oynatma zorlukları göz önünde bulundurulduğunda oldukça düşüktür. Performans açısından, gerçek sinyallerin kullanılması aldatmayı daha etkili kılarken, işlem gücüne bağlı olarak oluşan gecikmeler, performansı sınırlamakta ve orta seviyede tutmaktadır. Ancak, yüksek güçlü versiyonunda, karıştırma etkisinin ve aldatma mesafesinin artması performansı artırsa da bu artış, güç gereksinimleri ve buna bağlı olarak maliyeti de artırmaktadır.

Sahtecilik saldırılarının maliyeti ise sahte GPS sinyallerinin açık kaynaklı GPS-SDR-SIM kütüphanesi kullanılarak oluşturulması ve bu işlemin düşük işlem gücü gerektirmesi nedeniyle düşüktür. Uygulanabilirlik açısından, sahte GPS sinyallerinin basit bir şekilde elde edilmesi ve bu sinyallerin piyasada bulunabilen donanımlar ile hızlıca yayınlanabilmesi, yüksek bir uygulanabilirlik seviyesi sağlamaktadır. Ancak, CNR kontrollü sahtecilik aldatma saldırılarında, CNR'ın uygun seviyelerde kontrol edilmesi için gerekli olan güç çıkışının sağlanması maliyeti orta seviyeye çıkarmaktadır. Ayrıca, doğal sinyallerin seviyesinde CNR değerlerinin alıcı tarafından alınmasını sağlamak için yapılan ayarlamaların zorluğu, uygulanabilirliği düşük olarak değerlendirilmesine yol açmıştır. Performans kriterlerine göre, CNR kontrollü sahtecilik saldırıları aldatma tespitine karşı daha başarılı olsa da, genel aldatma performansı açısından sahtecilik saldırıları ile arasında belirgin bir fark gözlemlenmemiştir. Bu nedenle, her iki saldırının da performansı orta olarak değerlendirilmiştir.

Karıştırma sonrası aldatma saldırılarında, aldatma saldırısı öncesinde GPS L1 frekansı dışında kalan frekanslarda karıştırma yapılması gerekmektedir. Bu karıştırıcı sistemin kullanılması, karıştırma sonrası aldatma saldırısının maliyetini oldukça yüksek hale getirmektedir. Uygulanabilirlik, aldatma saldırısı öncesinde karıştırıcının devreye sokulması

ve önceden belirlenmiş bir karıştırma stratejisine göre ayarlanması gerekliliği nedeniyle orta olarak değerlendirilmiştir. Performans açısından, aldatma süresi boyunca karıştırma etkisinin yok sayılması durumunda, karıştırma sonrası alıcıda oluşturulan iç ortam etkisi sayesinde aldatma koşullarının kolayca sağlanabilmesi ve diğer saldırılara kıyasla daha fazla alıcıyı aldatabilmesi nedeniyle yüksek olarak değerlendirilmiştir.

Sonuç olarak, yeniden oynatma saldırıları genellikle ortalama maliyetli olmasına rağmen, yüksek güçlü versiyonları daha maliyetlidir. Sahtecilik saldırıları düşük maliyetli ve uygulanabilirliği yüksek olarak değerlendirilmektedir. Ancak, CNR kontrollü sahtecilik saldırıları, uygulanabilirliği düşük olmasına rağmen orta seviyede performans sergilemektedir. Karıştırma sonrası aldatma saldırıları ise yüksek maliyetli olmakla birlikte oldukça etkili sonuçlar doğurmaktadır.

Aldatma Yöntemi	**Karşı Tedbir Tekniği**	**Tespit Olasılığı**	**Güvenilirlik**
Yeniden Oynatma Saldırısı	CNR kontrol ile aldatma tespit	%60	Orta
	sVid kontrol ile aldatma tespit	%20	Düşük
	Doppler kayması kontrol ile aldatma tespit	%25	Düşük
Yüksek Güçlü Yeniden Oynatma Saldırısı	CNR kontrol ile aldatma tespit	%80	Yüksek
	sVid kontrol ile aldatma tespit	%20	Düşük
	Doppler kayması kontrol ile aldatma tespit	%20	Düşük
Sahtecilik Aldatma Saldırısı	CNR kontrol ile aldatma tespit	%50	Orta
	sVid kontrol ile aldatma tespit	%80	Yüksek
	Doppler kayması kontrol ile aldatma tespit	%60	Orta
CNR Kontrollü Aldatma Saldırısı	CNR kontrol ile aldatma tespit	%10	Düşük
	sVid kontrol ile aldatma tespit	%80	Yüksek
	Doppler kayması kontrol ile aldatma tespit	%60	Orta
Karıştırma Sonrası Aldatma Saldırısı	CNR kontrol ile aldatma tespit	%40	Orta
	sVid kontrol ile aldatma tespit	%30	Düşük
	Doppler kayması kontrol ile aldatma tespit	%25	Düşük

Tablo 5.4 Gerçeklenmiş Karşı Tedbir Yöntemlerinin Değerlendirilmesi

Tablo 5.4'te, her bir aldatma yöntemine karşı kullanılan karşı tedbir teknikleri, tespit olasılığı ve güvenilirlik açısından değerlendirilmiştir. Farklı ortamlarda gerçekleştirilen deneyler sonucunda tanımlanan aldatma saldırılarına karşı tedbir yöntemlerinin tespit olasılıkları hesaplanmıştır. Bu kapsamda, iç ortam ve farklı rakımlarda farklı CNR değerlerinin okunduğu dış ortamlarda deneyler yapılmıştır. Tespit yöntemlerinde kullanılan eşik değerleri, her bir deney için ortalama bir referans değere göre belirlenmiştir. Deneylerde, aldatma saldırılarına karşı tedbirlerin kaçında başarılı tespit yapıldığı ve kaçında hata yaptığı incelenmiş, bu bulgulara göre tespit yöntemlerinin güvenilirliği değerlendirilmiştir.

Yeniden oynatma saldırıları, daha önce kaydedilmiş doğal sinyallerin kullanılmasıyla gerçekleştirildiğinden, svid ve Doppler kayması parametreleri bu saldırıları tespit etmekte etkili olmamaktadır. Ancak, yayınlanan sinyalin RF katmanından geçmesi ve sinyal gücünde ani CNR değişimlerine yol açması, bu saldırıların tespit edilmesini kolaylaştırmaktadır. Yüksek güçlü versiyonlarında ise bu ani değişimlerin fark edilmesi daha da kolaylaşmaktadır.

Sahtecilik saldırılarında, uydu gruplarının ani değişimi ve yapay sinyal yayını nedeniyle saldırının tespiti nispeten daha kolaydır. Bununla birlikte, GPS-SDR-SIM kütüphanesinin Doppler etkisini hesaba katması ve CNR kontrolünün sağlanması, bu saldırıların tespit olasılığını azaltmıştır.

Karıştırma sonrası aldatma saldırılarında, karıştırma etkisi alıcının önceki bilgilerini yitirmesine neden olarak svid ve Doppler kaymasından yararlanmayı zorlaştırmaktadır. Ancak, karıştırma ve aldatma etkisinin CNR değerinde ani değişimlere yol açması, bu saldırıların tespit edilme olasılığını artırmaktadır.

Sonuç olarak yapılan analizler ışığında, her bir aldatma yöntemi için belirlenen karşı tedbirlerin etkinliği ve uygulanabilirliği değerlendirildiğinde, tespit olasılığı ve güvenilirlik açısından farklı sonuçlar elde edilmiştir. Yeniden oynatma saldırılarında, svid ve Doppler kayması gibi klasik tespit yöntemleri etkisiz kalmakta, ancak CNR değişimleri gibi parametreler sayesinde saldırının tespiti mümkün olabilmektedir. Sahtecilik saldırılarında, uydu gruplarının ani değişimi ve yapay sinyal yayını nedeniyle tespit olasılığı nispeten yüksek olmasına rağmen, Doppler etkisini hesaba katabilen gelişmiş saldırılar tespit zorluğunu artırmaktadır. Karıştırma sonrası aldatma saldırılarında ise, karıştırma etkisi alıcının önceki bilgilerini yitirmesine neden olsa da, CNR değerlerindeki ani değişimlerle tespit olasılığı artmaktadır.

Bu değerlendirmeler, gerçekleştirilen GPS aldatma ve karşı tedbir yöntemlerinin etkinliğini ve uygulanabilirliğini ortaya koymaktadır. Çalışmanın sonuçlarına dayanarak, en uygun karşı tedbirlerin seçilmesi ve uygulanması hedeflenmiştir.

Sonuç olarak bu çalışmada yapılan deneylerde aşağıdaki çıkarımlarda bulunulmuştur.

- Yapılan deneylerde Qualcomm Snapdragon 865 yonga seti gömülü, Exynos 990 yonga setine ve Exynos 1380 yonga setine gömülü GNSS alıcılarının, UBLOX M8N alıcısının, HERE2 alıcısının ve DJI Phantom 4 IHA'sına gömülü GNSS alıcısının iç ve dış ortamlarda yeniden oynatma aldatma saldırısı ve sahtecilik aldatma saldırılarının farklı stratejiler ile kullanılmasıyla aldatılabildiği gözlemlenmiştir.
- Yapılan deneylerde Apple A13 Bionic yonga setine gömülü GNSS alıcısının ve Septentrio AsteRx-m3 alıcısının kullanılan aldatma saldırısı yöntemleriyle aldatılamadığı gözlemlenmiştir.
- Dış ortamda yapılan deneylerde aldatma başarı oranı iç ortama göre çok daha düşüktür ve aldatılma süreleri daha uzundur.
- Doğal GNSS sinyallerinin olduğu ortamlarda A-GNSS özelliği bulunan alıcılarda yeniden oynatma saldırısının etkili olabilmesi için alıcının internet erişiminin kesilmesi gerekmektedir.
- Aldatma tekniklerinde yayınlanan sahte konum bilgisinin, gerçek konuma olan mesafesinin, kullanılan alıcılar için aldatma süresi performansına etkisi olmadığı gözlemlenmiştir.
- Sahtecilik aldatma tekniğinde yayınlanan sahte konumun hareketli olmasının aldatma süresi performansını etkilemediği gözlemlenmiştir.
- Aldatma tekniklerinin karıştırma sonrasında uygulanması aldatma olasılığını yükseltmektedir ve karşı tedbir yöntemlerine karşı etkili olmuştur.
- Farklı aldatma yöntemlerine farklı karşı tedbir yöntemleri daha etkili olmuştur.
- Yapılan deneylerde 1W'lık güç ile GNSS alıcılarının yaklaşık 600 metre mesafeden aldatılabildiği gözlemlenmiştir.

6 SONUÇ

Bu tez çalışması, Küresel Konumlandırma Sistemi (GPS) aldatma yöntemlerinin ve bu saldırılara karşı geliştirilen karşı tedbirlerin detaylı bir analizini ve karşılaştırmasını yapmayı amaçlamaktadır. GPS, modern dünyanın navigasyon, iletişim ve zamanlama gibi kritik alanlarında yaygın olarak kullanılan bir sistemdir. Ancak, bu sistemin güvenlik açıkları, aldatma ve karıştırma gibi saldırılara karşı savunmasız olmasına yol açmaktadır.

Tez kapsamında gerçekleştirilen deneyler ve simülasyonlar, GPS aldatma yöntemlerinin nasıl çalıştığını ve hangi durumlarda etkili olduğunu göstermiştir. Bu bağlamda, yeniden oynatma, sinyal üretimi ve güvenlik kodu tahmini gibi yaygın aldatma yöntemleri detaylı olarak incelenmiştir. Bu saldırıların, GNSS alıcılarını nasıl yanıltabildiği ve alıcıların konum, zaman ve navigasyon bilgilerini nasıl manipüle edebildiği gösterilmiştir.

İç ve dış ortam deneyleri, farklı aldatma senaryolarının alıcılar üzerindeki etkilerini değerlendirmek için kullanılmıştır. İç ortam deneylerinde, kontrollü koşullar altında GNSS alıcılarının yeniden oynatma saldırılarına maruz kaldığında nasıl tepki verdiği gözlemlenmiştir. Bu deneyler, kapalı bir ortamda gerçekleştirildiğinden, dış etkenlerin minimalize edilmesi sağlanmış ve daha kesin sonuçlar elde edilmiştir. Dış ortam deneylerinde ise gerçek GNSS sinyallerinin varlığı altında aldatma saldırılarının etkisi incelenmiştir. Bu deneyler, gerçek dünya koşullarında aldatma saldırılarının alıcılar üzerindeki etkisini değerlendirmemize olanak tanımıştır.

GPS aldatma saldırılarına karşı geliştirilen karşı tedbir yöntemleri, çeşitli parametreler göz önünde bulundurularak değerlendirilmiştir. Bu bağlamda, Taşıyıcı-Gürültü Oranı (CNR) izleme, uzay aracı kimlik kodu (sVid) kontrolü ve Doppler kayması izleme gibi yöntemler kullanılmıştır. Elde edilen sonuçlar, bu yöntemlerin aldatma saldırılarını tespit etmede ne kadar etkili olduğunu göstermiştir. Özellikle, CNR izleme ve Doppler kayması izleme yöntemleri, aldatma saldırılarını yüksek doğrulukla tespit edebilmiştir. Uzay aracı kimlik kodu kontrolü de etkili bir yöntem olarak öne çıkmıştır.

Deney sonuçları, GNSS alıcılarının çeşitli aldatma saldırılarına karşı savunmasız olduğunu ve bu saldırıların başarılı bir şekilde gerçekleştirilebileceğini göstermiştir. Özellikle İnsansız Hava Araçları'nın (İHA) ve cep telefonlarının GNSS alıcıları veya UBLOX GNSS alıcıları gibi yaygın olarak kullanılan alıcıların bu saldırılara karşı hassas olduğu tespit edilmiştir. Ancak, karşı tedbir olarak kullanılan parametrelerin doğru ve etkin bir şekilde uygulanması, aldatma saldırılarının tespit edilmesini ve engellenmesini sağlamaktadır. Bu tezde sunulan deneyler ve analizler, GPS aldatma saldırılarına karşı hangi karşı tedbirlerin en etkili olduğunu belirlemek için önemli bilgiler sağlamaktadır.

GNSS teknolojisinin sürekli gelişen yapısı ve aldatma tekniklerinin çeşitliliği göz önünde bulundurulduğunda, gelecekte daha kapsamlı çalışmaların yapılması gerekmektedir. Bu kapsamda, daha gelişmiş aldatma tekniklerinin incelenmesi, yeni karşı tedbir yöntemlerinin geliştirilmesi ve bu yöntemlerin farklı GNSS alıcıları üzerinde test edilmesi önem arz etmektedir. Özellikle, makine öğrenimi ve yapay zeka tekniklerinin kullanılarak dinamik ve adaptif karşı tedbir sistemlerinin geliştirilmesi, GNSS aldatma saldırılarına karşı daha güçlü ve etkili savunma stratejilerinin oluşturulmasına katkıda bulunacaktır.

Sonuç olarak, bu tez çalışması, GPS aldatma ve karşı tedbir yöntemlerinin etkinliğini ortaya koymuş ve gelecekte yapılacak çalışmalar için önemli bir temel oluşturmuştur. GNSS aldatma saldırılarına karşı alınabilecek önlemler konusunda sağlanan bilgiler, navigasyon sistemlerinin güvenliğinin artırılmasına yönelik önemli katkılar sunmaktadır.

KAYNAKLAR

[1] https://tr.wikipedia.org/wiki/K%C3%BCresel_uydu_seyr%C3%BCsefer_sistemi.

[2] https://www.e-education.psu.edu/geog862/l9.html.

[3] https://www.ettus.com/.

[4] Zhijun Wu, Yun Zhang, Yiming Yang, Cheng Liang, and Rusen Liu. Spoofing and anti-spoofing technologies of global navigation satellite system: A survey. *IEEE Access*, 8:165444–165496, **2020**.

[5] Umut Berkay Dokumacı and Baris Yuksekkaya. Analysis of global positioning system spoofing methods. In *2024 32nd Signal Processing and Communications Applications Conference (SIU)*, pages 1–4. IEEE, **2024**.

[6] A. El-Rabbany. *Introduction to GPS: The Global Positioning System*. Artech House mobile communications series. Artech House, **2002**. ISBN 9781580531832.

[7] National Research Council, Division on Engineering, Physical Sciences, Commission on Engineering, Technical Systems, Aeronautics, and Space Engineering Board. *The Global Positioning System: A Shared National Asset*. National Academies Press, **1995**. ISBN 9780309176446.

[8] M.S. Grewal, L.R. Weill, and A.P. Andrews. *Global Positioning Systems, Inertial Navigation, and Integration*. Wiley, **2007**. ISBN 9780470099711.

[9] Mark L Psiaki and Todd E Humphreys. GNSS spoofing and detection. *Proceedings of the IEEE*, 104(6):1258–1270, **2016**.

[10] Tae-Hee Kim, Cheon Sig Sin, Sanguk Lee, and Jae Hoon Kim. Analysis of performance of gps l1 signal generator in gps l1 signal. In *2014 14th*

International Conference on Control, Automation and Systems (ICCAS 2014), pages 1006–1009. IEEE, **2014**.

[11] Jahshan Bhatti and Todd E Humphreys. Hostile control of ships via false gps signals: Demonstration and detection. *NAVIGATION: Journal of the Institute of Navigation*, 64(1):51–66, **2017**.

[12] Komal Kumar Songala, Supraja Reddy Ammana, Hari Chandana Ramachandruni, and Dattatreya Sarma Achanta. Simplistic spoofing of GPS enabled smartphone. In *2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)*, pages 460–463. IEEE, **2020**.

[13] Bhaskara Satyanarayana Margana, Dattatreya Sarma Achanta, Komal Kumar Songala, and Supraja Reddy Ammana. A simple SDR based method to spoof low-end GPS aided drones for securing locations. In *2021 IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON)*, pages 32–36. IEEE, **2021**.

[14] Jabang Aru Saputro, Esa Egistian Hartadi, and Mohamad Syahral. Implementation of GPS attacks on dji phantom 3 standard drone as a security vulnerability test. In *2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE)*, pages 95–100. IEEE, **2020**.

[15] Tang Nguyen-Tan, Long Thai Hoang, An Khanh Nguyen, Tien Do Minh, Binh Bui-Thanh, and Nguyen TH Phuoc. GPS signal reception and spoofing based on software-defined radio devices. In *2022 RIVF International Conference on Computing and Communication Technologies (RIVF)*, pages 513–517. IEEE, **2022**.

[16] João Gaspar, Renato Ferreira, Pedro Sebastião, and Nuno Souto. Capture of UAVs through GPS spoofing. In *2018 Global Wireless Summit (GWS)*, pages 21–26. IEEE, **2018**.

[17] Hoan Nguyen Viet, Ki-Ryong Kwon, Soon-Kak Kwon, Eung-Joo Lee, Suk-Hwan Lee, and Chee-Yong Kim. Implementation of gps signal simulation for drone security using MATLAB/simulink. In *2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, pages 1–4. IEEE, **2017**.

[18] Pardhasaradhi Bethi, Srihari Pathipati, and P Aparna. Stealthy gps spoofing: Spoofer systems, spoofing techniques and strategies. In *2020 IEEE 17th India Council International Conference (INDICON)*, pages 1–7. IEEE, **2020**.

[19] Chris Rizos. Trends in gps technology & applications. In *2nd International LBS Workshop*. **2003**.

[20] Esat Elezi, Göksel Çankaya, Ali Boyacı, and Serhan Yarkan. The effect of electronic jammers on gps signals. In *2019 16th International Multi-Conference on Systems, Signals & Devices (SSD)*, pages 652–656. IEEE, **2019**.

[21] Ahmad Norhisyam Idris, Azman Mohd Suldi, Juazer Rizal Abdul Hamid, and Dinesh Sathyamoorthy. Effect of radio frequency interference (rfi) on the global positioning system (gps) signals. In *2013 IEEE 9th international colloquium on signal processing and its applications*, pages 199–204. IEEE, **2013**.

[22] Riddhi V Karpe and Sukanya Kulkarni. Software defined radio based global positioning system jamming and spoofing for vulnerability analysis. In *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, pages 881–888. IEEE, **2020**.

[23] Renato Ferreira, Joao Gaspar, Pedro Sebastiao, and Nuno Souto. Effective gps jamming techniques for uavs using low-cost sdr platforms. *Wireless Personal Communications*, 115:2705–2727, **2020**.

[24] Andrew J Kerns, Daniel P Shepard, Jahshan A Bhatti, and Todd E Humphreys. Unmanned aircraft capture and control via gps spoofing. *Journal of field robotics*, 31(4):617–636, **2014**.

[25] Todd E Humphreys, Jahshan A Bhatti, Daniel Shepard, and Kyle Wesson. The texas spoofing test battery: Toward a standard for evaluating gps signal authentication techniques. **2012**.

[26] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle. GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, 2012, **2012**.

[27] J Rossouw Van Der Merwe, Xabier Zubizarreta, Ivana Lukčin, Alexander Rügamer, and Wolfgang Felber. Classification of spoofing attack types. In *2018 European Navigation Conference (ENC)*, pages 91–99. IEEE, **2018**.

[28] Jonathan A Larcom and Hong Liu. Modeling and characterization of gps spoofing. In *2013 IEEE international conference on technologies for Homeland Security (HST)*, pages 729–734. IEEE, **2013**.

[29] Dingbo Yuan, Hong Li, Fei Wang, and Mingquan Lu. A gnss acquisition method with the capability of spoofing detection and mitigation. *Chinese Journal of Electronics*, 27(1):213–222, **2018**.

[30] Aleksandar Jovanovic, Cyril Botteron, and Pierre-Andre Fariné. Multi-test detection and protection algorithm against spoofing attacks on gnss receivers. In *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*, pages 1258–1271. IEEE, **2014**.

[31] Weikong Qi, Yu Zhang, and Xiaohui Liu. A gnss anti-spoofing technology based on doppler shift in vehicle networking. In *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 725–729. IEEE, **2016**.

[32] Ali Broumandan, Ali Jafarnia-Jahromi, Vahid Dehghanian, John Nielsen, and Gérard Lachapelle. Gnss spoofing detection in handheld receivers based on signal spatial correlation. In *Proceedings of the 2012 IEEE/ION position, location and navigation symposium*, pages 479–487. IEEE, **2012**.

[33] Leen A van Mastrigt, Ariën J van der Wal, and Patrick J Oonincx. Exploiting the doppler effect in gps to monitor signal integrity and to detect spoofing. In *2015 International Association of Institutes of Navigation World Congress (IAIN)*, pages 1–8. IEEE, **2015**.

[34] Jiaxun Tu, Xingqun Zhan, Maolin Chen, Han Gao, and Yuankang Chen. Gnss intermediate spoofing detection via dual-peak in frequency domain and relative velocity residuals. *IET Radar, Sonar & Navigation*, 14(3):439–447, **2020**.

[35] Ali Broumandan, Ali Jafarnia-Jahromi, Saeed Daneshmand, and Gérard Lachapelle. Overview of spatial processing approaches for gnss structural interference detection and mitigation. *Proceedings of the IEEE*, 104(6):1246–1257, **2016**.

[36] Ali Broumandan, Ali Jafarnia-Jahromi, Gérard Lachapelle, and Rigas T Ioannides. An approach to discriminate gnss spoofing from multipath fading. In *2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pages 1–10. IEEE, **2016**.

[37] Ali Broumandan, Ranjeeth Siddakatte, and Gérard Lachapelle. An approach to detect gnss spoofing. *IEEE Aerospace and Electronic Systems Magazine*, 32(8):64–75, **2017**.

[38] Daniele Borio. Panova tests and their application to gnss spoofing detection. *IEEE Transactions on Aerospace and Electronic Systems*, 49(1):381–394, **2013**.

[39] Daniele Borio and Ciro Gioia. A sum-of-squares approach to gnss spoofing detection. *IEEE Transactions on Aerospace and Electronic Systems*, 52(4):1756–1768, **2016**.

[40] Emanuela Falletti, Beatrice Motella, and Micaela Troglia Gamba. Post-correlation signal analysis to detect spoofing attacks in gnss receivers. In *2016 24th European Signal Processing Conference (EUSIPCO)*, pages 1048–1052. IEEE, **2016**.

[41] Patrick Y Hwang and Gary A McGraw. Receiver autonomous signal authentication (rasa) based on clock stability analysis. In *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*, pages 270–281. IEEE, **2014**.

[42] Dingbo Yuan, Hong Li, and Mingquan Lu. A method for gnss spoofing detection based on sequential probability ratio test. In *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*, pages 351–358. IEEE, **2014**.

[43] Fei Wang, Hong Li, and Mingquan Lu. Arpso-mle based gnss anti-spoofing method. In *2015 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, pages 1–5. IEEE, **2015**.

[44] Jason N Gross, Cagri Kilic, and Todd E Humphreys. Maximum-likelihood power-distortion monitoring for gnss-signal authentication. *IEEE Transactions on Aerospace and Electronic Systems*, 55(1):469–475, **2018**.

[45] Zhenjun Zhang, Xingqun Zhan, and Yanhua Zhang. Gnss spoofing localization based on differential code phase. In *2017 Forum on Cooperative Positioning and Service (CPGPS)*, pages 338–344. IEEE, **2017**.

[46] Hao Li and Xianbin Wang. Detection of gps spoofing through signal multipath signature analysis. In *2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–5. IEEE, **2016**.

[47] Khurram Ali, Esteban Garbin Manfredini, and Fabio Dovis. Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics. In *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*, pages 1240–1247. IEEE, **2014**.

[48] Wei Yimin, Li Hong, and Lu Mingquan. Spoofing profile estimation-based gnss spoofing identification method for tightly coupled mems ins/gnss integrated navigation system. *IET Radar, Sonar & Navigation*, 14(2):216–225, **2020**.

[49] Andrzej Felski. Methods of improving the jamming resistance of gnss receiver. *Annual of Navigation*, (23):185–198, **2016**.

[50] Yanfeng Hu, Shaofeng Bian, Bao Li, and Lei Zhou. A novel array-based spoofing and jamming suppression method for gnss receiver. *IEEE Sensors Journal*, 18(7):2952–2958, **2018**.

[51] Changhui Jiang, Shuai Chen, Yuwei Chen, Yuming Bo, Qingyuan Xia, and Boya Zhang. Analysis of the baseline data based gps spoofing detection algorithm. In *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, pages 397–403. IEEE, **2018**.

[52] F Wang, H Li, and M Lu. Gnss spoofing detection based on unsynchronized double-antenna measurements. ieee access, 6, 31203–31212, **2013**.

[53] Shuai Han, Lei Chen, Weixiao Meng, and Cheng Li. Improve the security of gnss receivers through spoofing mitigation. *IEEE Access*, 5:21057–21069, **2017**.

[54] Guanghui Xu, Feng Shen, Moeness Amin, and Chun Wang. Doa classification and ccpm-pc based gnss spoofing detection technique. In *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, pages 389–396. IEEE, **2018**.

[55] Saeed Daneshmand, Ali Jafarnia-Jahromi, Ali Broumandan, and Gérard Lachapelle. A gnss structural interference mitigation technique using antenna

array processing. In *2014 IEEE 8th sensor array and multichannel signal processing workshop (SAM)*, pages 109–112. IEEE, **2014**.

[56] Esteban Garbin Manfredini, Fabio Dovis, and Beatrice Motella. Validation of a signal quality monitoring technique over a set of spoofed scenarios. In *2014 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pages 1–7. IEEE, **2014**.

[57] Ali Jafarnia Jahromi, Ali Broumandan, Saeed Daneshmand, Gérard Lachapelle, and Rigas T Ioannides. Galileo signal authenticity verification using signal quality monitoring methods. In *2016 International Conference on Localization and GNSS (ICL-GNSS)*, pages 1–8. IEEE, **2016**.

[58] Zhenghao Zhang, Matthew Trinkle, Lijun Qian, and Husheng Li. Quickest detection of gps spoofing attack. In *MILCOM 2012-2012 IEEE Military Communications Conference*, pages 1–6. IEEE, **2012**.

[59] Yibing Li, Xiaochen Guo, Taige Zhang, and Qian Sun. Gps anti-spoofing algorithm based on improved particle filter. In *2018 USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)*, pages 17–18. IEEE, **2018**.

[60] Xiaomin Wei, Yao Wang, and Cong Sun. Perdet: machine-learning-based uav gps spoofing detection using perception data. *Remote Sensing*, 14(19):4925, **2022**.

[61] Yangjun Gao and Guangyun Li. A gnss instrumentation covert directional spoofing algorithm for uav equipped with tightly-coupled gnss/imu. *IEEE Transactions on Instrumentation and Measurement*, 72:1–13, **2023**.

[62] Tae-Hee Kim, Cheon Sig Sin, Sanguk Lee, and Jae Hoon Kim. Analysis of effect of anti-spoofing signal for mitigating to spoofing in gps l1 signal. In *2013 13th International Conference on Control, Automation and Systems (ICCAS 2013)*, pages 523–526. IEEE, **2013**.

[63] Silvio Semanjski, Alain Muls, Ivana Semanjski, and Wim De Wilde. Use and validation of supervised machine learning approach for detection of gnss signal spoofing. In *2019 International Conference on Localization and GNSS (ICL-GNSS)*, pages 1–6. IEEE, **2019**.

[64] Bin Yang, Mei Tian, Yawei Ji, Juan Cheng, Zongfu Xie, and Shuai Shao. Research on gnss spoofing mitigation technology based on spoofing correlation peak cancellation. *IEEE Communications Letters*, 26(12):3024–3028, **2022**.

[65] Erick Schmidt, Nikolaos Gatsis, and David Akopian. A gps spoofing detection and classification correlator-based technique using the lasso. *IEEE Transactions on Aerospace and Electronic Systems*, 56(6):4224–4237, **2020**.

[66] Jing Li, Jiantong Zhang, Shoufeng Chang, and Meng Zhou. Performance evaluation of multimodal detection method for gnss intermediate spoofing. *IEEE access*, 4:9459–9468, **2016**.

[67] Pai Wang, Yongqing Wang, Ediz Cetin, Andrew Graham Dempster, and Siliang Wu. Gnss jamming mitigation using adaptive-partitioned subspace projection technique. *IEEE Transactions on Aerospace and Electronic Systems*, 55(1):343–355, **2018**.

[68] Kun Dong, Zilong Zhang, and Xiaodong Xu. A hybrid interference suppression scheme for global navigation satellite systems. In *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, pages 1–7. IEEE, **2017**.

[69] Esteban Garbin Manfredini, Dennis M Akos, Yu-Hsuan Chen, Sherman Lo, Todd Walter, and Per Enge. Effective gps spoofing detection utilizing metrics from commercial receivers. In *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, pages 672–689. **2018**.

[70] Daniele Borio. A multi-state notch filter for gnss jamming mitigation. In *International Conference on Localization and GNSS 2014 (ICL-GNSS 2014)*, pages 1–6. IEEE, **2014**.

[71] GNSS Inside. Nobody's fool: Spoofing detection in a high-precision receiver. *Inside GNSS-Global Navigation Satellite Systems Engineering, Policy, and Design, Available: https://insidegnss. com/nobodys-fool-spoofing-detection-in-a-high-precision-receiver*, **2020**.

[72] Gianluca Caparra and Nicola Laurenti. On the use of csk for gnss anti-spoofing. In *2018 9th ESA Workshop on Satellite NavigationTechnologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pages 1–7. IEEE, **2018**.

[73] Mukhtar Ahmad, Muhammad Atif Farid, Sheeraz Ahmed, Khalid Saeed, M Asharf, and Usman Akhtar. Impact and detection of gps spoofing and countermeasures against spoofing. In *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pages 1–8. IEEE, **2019**.

[74] Yan Guo, Meiping Wu, Kanghua Tang, Junbo Tie, and Xian Li. Covert spoofing algorithm of uav based on gps/ins-integrated navigation. *IEEE Transactions on Vehicular Technology*, 68(7):6557–6564, **2019**.

[75] Shou-Sheu Lin and Yu-Hao Li. A sdr-based gps receiver with low accuracy of local oscillator. In *2021 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, pages 1–2. IEEE, **2021**.

[76] Paresh Risbud, Nikolaos Gatsis, and Ahmad Taha. Vulnerability analysis of smart grids to gps spoofing. *IEEE Transactions on Smart Grid*, 10(4):3535–3548, **2018**.

[77] Mattia Berardo, Esteban Garbin Manfredini, Fabio Dovis, and Letizia Lo Presti. A spoofing mitigation technique for dynamic applications. In *2016 8th ESA*

Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), pages 1–7. IEEE, **2016**.

[78] Sriramya Bhamidipati, Tara Yasmin Mina, and Grace Xingxin Gao. Gps time authentication against spoofing via a network of receivers for power systems. In *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, pages 1485–1491. IEEE, **2018**.

[79] Ali Khalajmehrabadi, Nikolaos Gatsis, David Akopian, and Ahmad F Taha. Real-time rejection and mitigation of time synchronization attacks on the global positioning system. *IEEE Transactions on Industrial Electronics*, 65(8):6425–6435, **2018**.

[80] Nathaniel Carson, Scott M Martin, Joshua Starling, and David M Bevly. Gps spoofing detection and mitigation using cooperative adaptive cruise control system. In *2016 IEEE Intelligent Vehicles Symposium (IV)*, pages 1091–1096. IEEE, **2016**.

[81] Shuai Han, Desi Luo, Weixiao Meng, and Cheng Li. A novel anti-spoofing method based on particle filter for gnss. In *2014 IEEE International Conference on Communications (ICC)*, pages 5413–5418. IEEE, **2014**.

[82] Shunshun Shang, Hong Li, Chenxi Peng, and Mingquan Lu. A novel method for gnss meaconer localization based on a space–time double-difference model. *IEEE Transactions on Aerospace and Electronic Systems*, 56(5):3432–3449, **2020**.

[83] Kyle D Wesson, Brian L Evans, and Todd E Humphreys. A combined symmetric difference and power monitoring gnss anti-spoofing technique. In *2013 IEEE Global Conference on Signal and Information Processing*, pages 217–220. IEEE, **2013**.

[84] Yang Gao, Hong Li, Mingquan Lu, and Zhenming Feng. Intermediate spoofing strategies and countermeasures. *Tsinghua Science and Technology*, 18(6):599–605, **2013**.

[85] Marco Ceccato, Francesco Formaggio, Nicola Laurenti, and Stefano Tomasin. Generalized likelihood ratio test for gnss spoofing detection in devices with imu. *IEEE Transactions on Information Forensics and Security*, 16:3496–3509, **2021**.

[86] `https://cddis.nasa.gov/archive/gnss/data/daily/`.