T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

İNSANSIZ HAVA ARAÇLARINDA GPS KARIŞTIRMA YÖNTEMLERİ VE ANALİZİ

Mehmet ÇIRAK

Yüksek Lisans Tezi

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI

TEMMUZ 2025

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

İNSANSIZ HAVA ARAÇLARINDA GPS KARIŞTIRMA YÖNTEMLERİ VE ANALİZİ

Tez Yazarı
Mehmet ÇIRAK

Danışman
Doç. Dr. Orhan YAMAN

TEMMUZ 2025
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	İnsansız Hava Araçlarında GPS Karıştırma Yöntemleri ve Analizi
Yazarı:	Mehmet ÇIRAK
İlk Teslim Tarihi:	17.06.2025
Savunma Tarihi:	17.07.2025

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

	İmza	
Danışman:	Doç. Dr. Orhan YAMAN Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Başkan:	Doç. Dr. İlhan Fırat KILINÇER Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Üye:	Dr. Öğr. Üyesi Huzeyfe Muhammed KOCABAŞ Amasya Üniversitesi, Mühendislik Fakültesi	Onayladım

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Burhan ERGEN
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "İnsansız Hava Araçlarında GPS Karıştırma Yöntemleri ve Analizi" Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

17.07.2025

Mehmet ÇIRAK

ÖNSÖZ

"İnsansız Hava Araçlarında GPS Karıştırma Yöntemleri ve Analizi" başlıklı yüksek lisans tezimi hazırlarken gerek literatürde bu alanda fazla çalışma olmaması gerek bu alanın hayatımıza yeni yeni girmesinden dolayı literatür taraması ve araştırmalarımda bir hayli gayret sarf ettik. Ama çalışmalarımı yönlendiren, çalışma aşamasında desteklerini esirgemeyen ve beni motive eden danışman hocam Sayın Doç. Dr. Orhan YAMAN'a teşekkürü borç bilirim.

Çalışmalarımın gerçekleşmesinde katkıları olan Fırat Üniversitesi Adli Bilişim Mühendisliği Anabilim Dalı öğretim üyelerine teşekkür ederim.

Ayrıca bu süreçte özverili bir şekil de yanımda olan ve maddi manevi desteklerini esirgemeyen aileme teşekkür ederim.

Mehmet ÇIRAK
ELAZIĞ, 2025

İÇİNDEKİLER

Sayfa

ÖZET

İnsansız Hava Araçlarında GPS Karıştırma Yöntemleri ve Analizi

Mehmet ÇIRAK

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Adli Bilişim Mühendisliği Anabilim Dalı

Temmuz 2025, Sayfa: x + 35

GPS (Global Positioning System) karıştırma tekniği, İnsansız Hava Araçlarının (İHA) kontrol sinyallerini veya veri aktarımını bozmak için kullanılan en temel yöntemlerden biridir. Bu yöntemde, İHA ile kontrol istasyonu arasındaki iletişimi sağlayan RF (radyo frekansı) sinyallerine geniş bantlı gürültü eklenmektedir. Bu, sinyal-gürültü oranını düşürüp iletişimi zorlaştırmakta veya imkansız hale getirmektedir. Özellikle otonom veya yarı otonom İHA'lar için, bu gürültü engelleme tekniği büyük bir risk oluşturabilir. Çünkü bu İHA'lar daha az insan müdahalesine gereksinim duyarlar. RF sinyallerine gürültü ekleyerek, İHA'nın alıcı tarafından gönderilen komutları doğru bir şekilde almasını engelleyebilir ve bu da İHA'nın güvenliğini tehlikeye atabilir. Gürültü engelleme ve GNSS engelleme gibi yöntemlerin etkinliğini azaltmak için farklı İHA'lar farklı iletişim teknolojileri ve güvenlik önlemleri kullanabilirler. Ancak, bu tür saldırılar hala ciddi bir tehdit oluşturmakta ve İHA'ların güvenliğini sağlamak için sürekli olarak gelişen savunma stratejileri ve teknolojileri gerektirmektedir. Bu çalışmada İHA'larda GPS karıştırma yöntemleri incelenmiş ve karşılaştırılmıştır. GPS sinyal sistemleri bileşenleri ve çalışma yapısı incelenmiştir. GPS karıştırma yöntemleri araştırılmış ve bu yöntemler için simülasyonlar gerçekleştirilmiştir. Tez kapsamında Noise Jamming, Tone Jamming, Swept Jamming, Follower Jamming, Smart Jamming ve GNSS Jamming yöntemleri incelenmiştir. Öncelikle simülasyon ortamında bütün jamming yöntemleri modellenmiştir. Daha sonra farklı senaryolarda jamming yöntemlerinin performans değerlendirmesi yapılmıştır. Özellikle jamming katsayıları değiştirilerek GPS ve PSD grafikleri elde edilmiştir. Bir İHA'nın belirli bir lokasyonda hareketi simüle edilmiş, jamming yöntemleri sırasıyla uygulanmış ve rota sapma oranları hesaplanmıştır. Bu kapsamda; Follower Jamming ve Noise Jamming türlerinin GPS sinyalleri üzerindeki etkisi diğer jamming türlerine göre daha fazla olduğu gözlemlenmiştir.

Anahtar Kelimeler: İHA, GPS, Karıştırma, Savunma sistemleri

ABSTRACT

GPS Jamming Methods and Analysis in Unmanned Aerial Vehicles

Mehmet ÇIRAK

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Digital Forensic Engineering

July 2025, Pages: x + 35

GPS (Global Positioning System) jamming is one of the most fundamental methods used to disrupt control signals or data transmissions of Unmanned Aerial Vehicles (UAVs). This method adds broadband noise to the RF (radio frequency) signals that enable communication between the UAV and the control station. This reduces the signal-to-noise ratio, making communication difficult or impossible. This noise cancellation technique can pose a significant risk, especially for autonomous or semi-autonomous UAVs, as these UAVs require less human intervention. By adding noise to the RF signals, it can prevent the UAV from correctly receiving commands sent by the receiver, compromising the UAV's security. Different UAVs may employ different communication technologies and security measures to mitigate the effectiveness of methods such as noise cancellation and GNSS jamming. However, such attacks still pose a serious threat and require continuously evolving defense strategies and technologies to ensure UAV security. This study examines and compares GPS jamming methods in UAVs. The components and operational structure of GPS signal systems are examined. GPS jamming methods were investigated and simulations were conducted for these methods. This thesis examined Noise Jamming, Tone Jamming, Swept Jamming, Follower Jamming, Smart Jamming, and GNSS Jamming. First, all jamming methods were modeled in a simulation environment. Then, the performance of the jamming methods was evaluated in different scenarios. Specifically, GPS and PSD graphs were obtained by varying the jamming coefficients. The movement of a UAV at a specific location was simulated, jamming methods were applied sequentially, and course deviation rates were calculated. In this context, it was observed that Follower Jamming and Noise Jamming had a greater impact on GPS signals than other jamming types.

Keywords: UAV, GPS, Jamming, Defence Systems

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Simgeler

C/A Kodu : Kaba Yakalama Kodu (Coarse /Aquisition Code)
P Kodu : Hassas Kod (Precise Code)

Kısaltmalar

BER : Bit Hata Oranı
GNSS : Küresel Navigasyon Uydu Sistemi (Global Navigation Satellite Systems)
GPS : Küresel Konumlama Sistemi (Global Positioning System)
HALE : Yüksek Yükseklik Uzun Menzil
İHA : İnsansız Hava Aracı
LEO : Düşük Dünya Yörüngesi
MALE : Orta Yükseklik Uzun Menzil
MEO : Orta Dünya Yörüngesi
PRN : Sözde Rastgele Gürültü (Pseudo Random Noise)
PSD : Güç Spektral Yoğunluğu
RF : Radyo Frekans
RFIC : Radyo Frekansı Entegre Devre
SAR : Sentetik Açıklıklı Radar
SNR : Sinyal Gürültü Oranı(Signal Noise Ratio)
SVN : Uzay Aracı Numarası (Space Vehicle Number)
VTOL : Dikey Kalkış ve İniş (Vertical Take-Off Landing)

1. GİRİŞ

İnsansız Hava Araçları (İHA'lar), günümüzde teknolojinin en hızlı gelişim gösterdiği alanlardan biri haline gelmiştir. Hem sivil hem de askeri uygulamalarda sağladığı avantajlar nedeniyle İHA'lara olan ilgi ve yatırım, küresel ölçekte giderek artmaktadır. Uygun maliyetli çözümler sunmaları, riskli görevlerde insan hayatını tehlikeye atmadan görev yapabilmeleri ve çeşitli sensörlerle donatılarak çok sayıda işlevi aynı anda yerine getirebilmeleri, bu teknolojinin farklı alanlarda benimsenmesini kolaylaştırmıştır. Keşif, gözetleme, haritalama, kargo taşımacılığı, trafik izleme, sınır güvenliği, doğal afet sonrası durum tespiti, yangınla mücadele, tarımsal analiz ve arama-kurtarma operasyonları gibi geniş bir kullanım yelpazesi, İHA'ların stratejik önemini her geçen gün daha da artırmaktadır.

İHA'ların bu denli yaygınlaşması beraberinde teknik, etik, hukuki ve güvenlik temelli birçok tartışmayı da gündeme getirmiştir. Özellikle güvenlik açısından, bu sistemlerin dış müdahalelere açık olması, hem görev etkinliğini azaltmakta hem de ciddi zarar ve kayıplara yol açabilecek riskleri beraberinde getirmektedir. Bu bağlamda, İHA'ların konumlama ve navigasyon sistemlerinin güvenliği en kritik hususlardan biri olarak öne çıkmaktadır. İHA'ların büyük çoğunluğu, yönlerini tayin etmek ve görev planlarını icra edebilmek için **Global Konumlandırma Sistemi (GPS)** gibi uydu tabanlı konumlama teknolojilerine bağımlıdır. GPS, sistemin hem uçuş kontrolünü hem de hedef bölgeye yönlendirilmesini sağlamak açısından hayati bir bileşen olarak değerlendirilmektedir.

Ancak, GPS sisteminin en zayıf yönlerinden biri, yaydığı sinyallerin düşük güçlü olması ve bu sinyallerin hem çevresel koşullar hem de kötü niyetli müdahaleler karşısında kolayca bozulabilmesidir. GPS sinyallerinin engellenmesi ya da karıştırılması, İHA'nın bulunduğu konumu yanlış algılamasına, rota dışına çıkmasına, kontrolün kaybedilmesine ya da görevin tamamen başarısızlıkla sonuçlanmasına neden olabilir. Özellikle askeri operasyonlar gibi zaman ve doğruluk açısından yüksek hassasiyet gerektiren uygulamalarda bu tür bir karıştırma, yalnızca teknik bir sorun değil; aynı zamanda stratejik ve taktik düzeyde ciddi bir tehdit haline gelmektedir.

GPS karıştırma (jamming) teknikleri, temel olarak uydu sinyallerine müdahale ederek bu sinyallerin alıcı cihazlar tarafından algılanmasını ve kullanılmasını engelleme prensibine dayanmaktadır. Bu işlem genellikle **radyo frekansı (RF)** spektrumuna geniş bantlı parazit (gürültü) sinyalleri gönderilerek gerçekleştirilir. GPS sinyallerinin taşıdığı bilgi, bu parazit sinyalleri nedeniyle alıcı tarafından işlenemez hale gelir ve İHA'nın konumlama yetisi kaybolur. Bununla birlikte, sadece sinyal engelleme değil; aynı zamanda sahte sinyaller göndererek İHA'yı yanlış yönlere sevk etmeye dayalı **spoofing** saldırıları da modern elektronik harp teknolojisinin bir parçası haline gelmiştir. Tüm bu müdahale yöntemleri, otonom veya yarı otonom sistemlerde insan faktörünün sınırlı olması nedeniyle daha da yıkıcı sonuçlara neden olabilir.

Özellikle savunma sanayii açısından bakıldığında, İHA'ların GPS sinyallerine bu kadar bağımlı olması, elektronik harp ortamlarında ciddi bir zafiyet olarak değerlendirilmektedir. Bu nedenle, hem saldırı tekniklerini anlamak hem de bu saldırılara karşı etkili savunma mekanizmaları geliştirmek, günümüz güvenlik stratejilerinde kritik bir öncelik haline gelmiştir. Aynı şekilde, sivil kullanımda da GPS karıştırma nedeniyle ortaya çıkabilecek yön kaybı, düşme, çarpışma gibi riskler yalnızca ekonomik değil, aynı zamanda can güvenliğini de tehdit etmektedir.

Bu çalışmada, İHA'ların görev başarısını ve operasyonel güvenliğini tehdit eden GPS karıştırma teknikleri detaylı olarak ele alınacaktır. Öncelikle GPS sisteminin yapısı, işleyiş prensipleri ve İHA sistemleriyle olan ilişkisi açıklanacak; ardından jamming, spoofing ve meaconing gibi sinyal bozma yöntemleri teknik yönleriyle incelenecektir. Bu saldırıların İHA operasyonları üzerindeki potansiyel etkileri; kontrol kaybı, yön sapması, görev iptali ve sistem hasarı gibi sonuçlar bağlamında değerlendirilecektir. Ayrıca, GPS karıştırmalara karşı geliştirilen savunma stratejileri, alternatif navigasyon çözümleri (INS, görsel odometri, manyetik pusula vb.) ve yapay zekâ destekli konumlama sistemleri gibi modern teknolojiler de tartışma konusu yapılacaktır.

Bu çalışmanın temel amacı, İHA'lar için hayati öneme sahip konumlama güvenliğini tehdit eden karıştırma girişimlerine dair farkındalığı artırmak ve bu alanda çalışan mühendisler, güvenlik uzmanları, İHA operatörleri ve akademisyenler için kapsamlı bir bilgi kaynağı oluşturmaktır. Aynı zamanda, gelecekte daha güvenli ve dirençli İHA sistemlerinin geliştirilmesi adına katkı sağlamak hedeflenmektedir. GPS karıştırma gibi dış müdahalelere karşı dayanıklı sistemlerin tasarımı, yalnızca teknik bir başarı değil; aynı zamanda ulusal güvenlik, kamu güvenliği ve ekonomik sürdürülebilirlik açısından da stratejik bir zorunluluk haline gelmiştir.

1.1. Literatür Özeti

GPS'ye karşı tehditlerin ciddiyeti konusundaki farkındalık arttıkça, bu konudaki araştırmalar son yıllarda büyük ölçüde hız kazanmıştır. Araştırmalar genellikle tespit tekniklerine odaklanmış olsa da GPS aldatma teknikleri de GPS alıcılarının zayıf noktalarını belirlemek için yoğun bir şekilde araştırılmaktadır. Zayıf noktaların belirlenmesiyle, daha sağlam navigasyon çözümlerine sahip sistemler tasarlanabilir. Bu konuda birçok çalışma bulunmaktadır. [1]'de yazarlar, okuyucuları en son aldatma vakaları hakkında bilgilendirmiş ve aldatma tehlikelerine vurgu yapmışlar, ardından aldatma ve saldırı yöntemlerini kullanılan teknolojilere göre sınıflandırma yaparak çeşitli senaryolarda nasıl kullanılabileceklerini tartışmışlardır. Ayrıca, makale aldatma tespit yöntemlerini sınıflandırmakta ve saldırı yöntemlerinin çeşitli yöntemlere karşı etkinliğini tartışmaktadır. Makalede anlatılan tespit yöntemleri hem navigasyon düzeyinde, hem şifreleme düzeyinde hem de ön korelasyon düzeyinde verilir. Makale, bahsedilen tespit yöntemlerinin analitik arka planını kısaca paylaşmaktadır. Son olarak, makale, aldatma saldırısının alıcı sistemini nasıl etkilediğine bağlı olarak kurtarma yöntemlerini

incelemekte ve aldatma sonrası otantik sinyallerin kurtarılması ve doğrulanması adımlarını tanıtmaktadır.

Başka bir makale [2], öncelikle aldatma vakaları hakkında dikkat çekerek durumun önemi hakkında bilgi verilmiştir. Makale, aldatma oluşturma tekniklerini üç alt kategoriye ayırmış ve bu teknikler arasındaki net bir çerçeve çizmiştir. Her birine karşı olası karşı önlem yöntemlerini kısaca tanıtmıştır. Ayrıca, GPS'nin aldatma saldırılarına karşı zayıf noktalarını, navigasyon ve pozisyon düzeyindeki zayıflıklar, veri biti düzeyinde ve sinyal işleme düzeyindeki zayıflıklar olmak üzere üç kategoride sınıflandırmaktadır. Bu sınıflandırma, sinyal işleme düzeyindeki zayıflıkların uygun sinyal işleme teknikleri kullanılarak önlenmesi ve navigasyon çözümü düzeyindeki zayıflıkların tutarlılık kontrolleri kullanılarak önlenmesi gibi, tespit yöntemlerinin sınıflandırılmasını kolaylaştırmaktadır. Aldatma önleme tekniklerini sınıflandırmadan önce, makale, aldatma varlığında analitik olarak alınan sinyal modelini türetmekte ve daha sonra tespit ve hafifletme olmak üzere ana iki aldatma önleme tekniği kategorisini tanıtmaktadır. Yazarlar, aldatma tespit teknikleri için on ana kategori tanımlamakta ve her biri için alıcıdan toplanan farklı bilgilere göre alt kategorileri tekrar tanıtarak geniş bilgi vermektedir. Ayrıca, makale, tespit tekniklerini karmaşıklık düzeylerine, etkinlik ve farklı aldatma senaryolarına karşı kapsama düzeylerine göre araştırmakta ve sınıflanmaktadır. Yazarlar, hafifletme tekniklerini üç gruba ayırmış ve aynı şekilde incelemelerini yapmışlardır. Son olarak, makale aldatmaya karşı test senaryolarını tanıtmakta ve GPS sinyallerinin dışarıda iletilmesini kesinlikle yasaklayan kuralları vurgulamaktadır.

[3]'de yazar, aldatma saldırılarının arkasındaki olası motivasyonları paylaşmış ve diğer çalışmalardan farklı olarak aldatma saldırılarını ve tespit yöntemlerini sınıflandırmıştır. Makale, alıcı durumuna ilişkin üç farklı senaryo tanıtmıştır. Bunlar soğuk başlatma, yeniden edinme ve izleme modları olarak sınıflandırılır. Soğuk başlatma modunda, alıcının konumu, zamanı, efemeris ve almanak hakkında önceden bilgisi yoktur. Aldatmanın en fazla bağımsızlık verdiği ve dolayısıyla daha kolay aldatma yapılabileceği belirtilmiştir. Yeniden edinme modunda, aldatma edinmeden önce başlar, ancak alıcının önceden bilgisi vardır. Bu senaryo, aldatma işleminden önce bir tıkanıklık varlığında meydana gelir. Son senaryo, aldatmanın en zorlu durumu olarak belirtilir. Bu makalede yapılan diğer farklı sınıflandırma, aldatma sinyallerinin alıcıya enjekte edilmesiyle ilgilidir. Koherentsiz üst üste enjeksiyon yönteminde, makale, otantik sinyallerin gürültü altında tutulabileceğini ve koherent üst üste enjeksiyon yönteminde, aldatmanın alıcının tam konumunu bilmesi gerektiğini belirtir. Makale, tanıtılan her yöntemin etkinliğini araştırır.

Başka bir makalede [4], bu konuda önceki makalelerin modası geçmiş olduğunu iddia etmiş ve son dönemdeki ilerlemeleri tam olarak kapsamadığını belirtmiştir. Makale, esas olarak hava araçlarına karşı aldatma tehditlerine odaklanmış olup kara platformlarına karşı tehditlerden kısaca bahsetmiştir.

Önceki makalelerin aksine, konunun analitik arka planından çok pratik gerçek hayat endişeleri incelenmiştir. Tehditler aldatma ve karıştırma olarak sınıflandırılır. Aldatma saldırıları, zaman ve konum aldatması olarak sınıflandırılır. Aldatma saldırıları, aldatma vericisinin alıcıya göre konumuna ve gizliliğine göre yorumlanır. Makaleye göre, aldatma saldırılarının gizliliği, açık saldırı ve gizli saldırı olmak üzere iki kategoriye ayrılır. Açık saldırılarda, saldırı gizlemeye çalışılmaz. Ayrıca, makale başarılı aldatma saldırılarına karşı karşılaşılan zorlukları inceler ve makaleyi bu konuda çözülmemiş sorunları ve gelecek araştırma yönlerini tartışarak sonlandırır.

1.2.Tezin Amacı ve Konusu

İnsansız Hava Araçları günümüzde yaygın hale gelmiş ve birçok alanda kullanılır hale gelmiştir. Bu çalışmada İHA'ların konum belirleme ve navigasyon sistemlerinde GPS ve benzeri sistemler kullanılmakta ve bu sistemler dışarıdan saldırılara açık sistemlerdir. Bu çalışmada İHA'larda GPS sistemi, GPS karıştırması ve etkileri incelenmiş ve İHA Pilotları ve İHA alanında çalışma yapan personele konunun öneminin anlatılması amaçlanmıştır.

2. İNSANSIZ HAVA ARAÇLARI

İnsansız Hava Araçları (İHA'lar), içinde insan bulunmaksızın uzaktan kumanda edilebilen ya da önceden programlanmış görevleri otonom olarak yerine getirebilen hava araçlarıdır. İlk olarak 20. yüzyılın başlarında askeri keşif ve gözetleme faaliyetleri için geliştirilen İHA'lar, günümüzde hem askeri hem de sivil amaçlarla çok çeşitli görevlerde kullanılmaktadır [5]. İHA sistemleri, uçuş kontrol sistemi, yer kontrol istasyonu, iletişim altyapısı ve faydalı yüklerden (kamera, radar, sensör vb.) oluşan kompleks bir yapıya sahiptir.

İHA teknolojisinin tarihi, 1. Dünya Savaşı'na kadar uzanmakta olup, o dönemde hedef uçağı olarak kullanılan ilkel sistemlerle başlamıştır. 1990'lı yıllarda ABD'nin "Predator" sınıfı İHA'ları geliştirmesiyle birlikte, insansız sistemler hem istihbarat hem de operasyonel görevlerde etkin olarak kullanılmaya başlanmıştır. Son yıllarda teknolojik gelişmelerle birlikte boyutları küçülen ve daha düşük maliyetli hale gelen İHA'lar, sadece devlet kurumlarının değil, özel sektör ve bireysel kullanıcıların da hizmetine sunulmuştur [6].

İHA'lar, çok çeşitli uygulama alanlarında kullanılmaktadır. Askeri uygulamalar arasında keşif, gözetleme, sınır güvenliği, hedef tespiti ve hassas saldırılar yer alırken; sivil alanda tarım, çevresel izleme, haritalama, afet yönetimi, trafik kontrolü, enerji hatlarının denetimi ve kargo taşımacılığı gibi alanlarda aktif olarak görev yapmaktadır [7]. Tarımsal İHA'lar ile bitki sağlığı izlenebilmekte, afet İHA'ları ile depremler veya yangınlar sonrası hızlı müdahale sağlanabilmektedir. Şekil 2.1'de TUSAŞ tarafından üretilen Aksungur İHA gösterilmiştir.

Şekil 2.1. İnsansız Hava Aracı

İHA'lar ağırlık, irtifa, menzil, kanatlar ve rotorlar ile uygulama alanları temelinde sınıflandırılmıştır. Genel olarak tek bir sınıflandırma standardı yoktur. Bununla birlikte, genel olarak literatürde yapılan sınıflandırma çeşitleri aşağıdaki gibidir [8]. Bazı sınıflandırmalara ait örnek İHA'lar şekil 2.2'de görülmektedir.

Şekil 2.2. İHA'ların Sınıflandırılması

2.1. Ağırlığa Göre

Nano: 250 gramdan az ağırlığa sahip İHA'lar

Mikro: 250 gramdan fazla ve 2 kilogramdan az ağırlığa sahip İHA'lar

Küçük: 2 kilogramdan fazla ve 25 kilogramdan az ağırlığa sahip İHA'lar

Orta: 25 kilogramdan fazla ve 150 kilogramdan az ağırlığa sahip İHA'lar

Büyük: 150 kilogramdan fazla ağırlığa sahip İHA'lar

2.2. İrtifaya ve Menzile Göre

Elde Taşınabilir: 600 m'den az yükseklikte uçabilen ve 2 km'den az menzile sahip İHA'lar.

Yakın: 1500 m'den az yüksekliğe ve 10 km'den az menzile sahip İHA'lar.

NATO: 3000 m'den az yüksekliğe ve 50 km'den az menzile sahip İHA'lar.

Taktiksel: 5500 m'den az yüksekliğe ve 160 km'den az menzile sahip İHA'lar.

MALE (Orta Yükseklik Uzun Menzil): 9100 m'den az yüksekliğe ve 200 km'den az menzile sahip İHA'lar.

HALE (Yüksek Yükseklik Uzun Menzil): 9100 m'den fazla yükseklikte ve belirsiz menzile sahip İHA'lar.

Hipersonik: Yaklaşık 15200 m yükseklikte ve 200 km'den fazla menzile sahip İHA'lar.

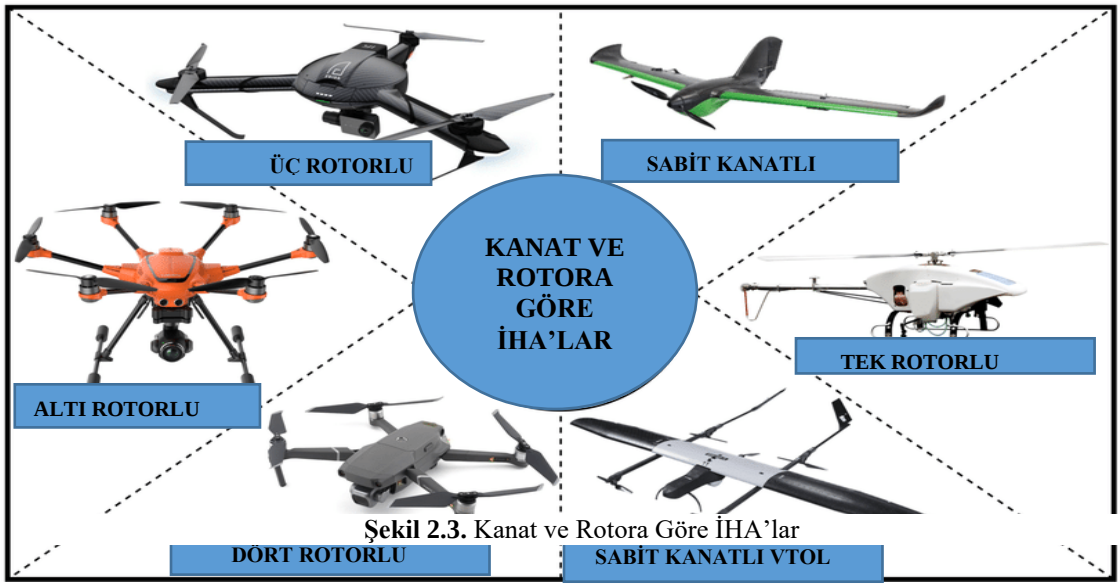
2.3. Kanat ve Rotora Göre

Sabit Kanatlı: Sabit kanatlara sahip bir uçak tasarımına benzeyen İHA'lar.

Tek Rotorlu: Bir ana rotor ve kuyrukta başka bir küçük rotoru olan bir helikopter tasarımına benzeyen İHA'lar.

Çoklu Rotorlu: Birden fazla rotoru olan İHA'lar. En yaygın olanları üç rotorlu (tricopter), dört rotorlu (quadcopter), altı rotorlu (hexacopter) ve sekiz rotorlu (octacopter) olanlardır.

Sabit Kanatlı Hibrit VTOL: Daha uzun uçuş süresine sahip hibrit İHA'lar. Sabit kanatlı İHA'ların istikrarına ve aynı zamanda dikey olarak kalkış yapma ve iniş yapma yeteneğine sahiptirler. Burada, VTOL dikey kalkış ve iniş anlamına gelir. Şekil 2.3'te bu kategorideki çeşitli İHA'lara örnek verilmiştir.



Şekil 2.3. Kanat ve Rotora Göre İHA'lar

2.4. Uygulamaya Göre

Kişisel: Video çekimi ve eğlence gibi uygulamalar için kullanılır.

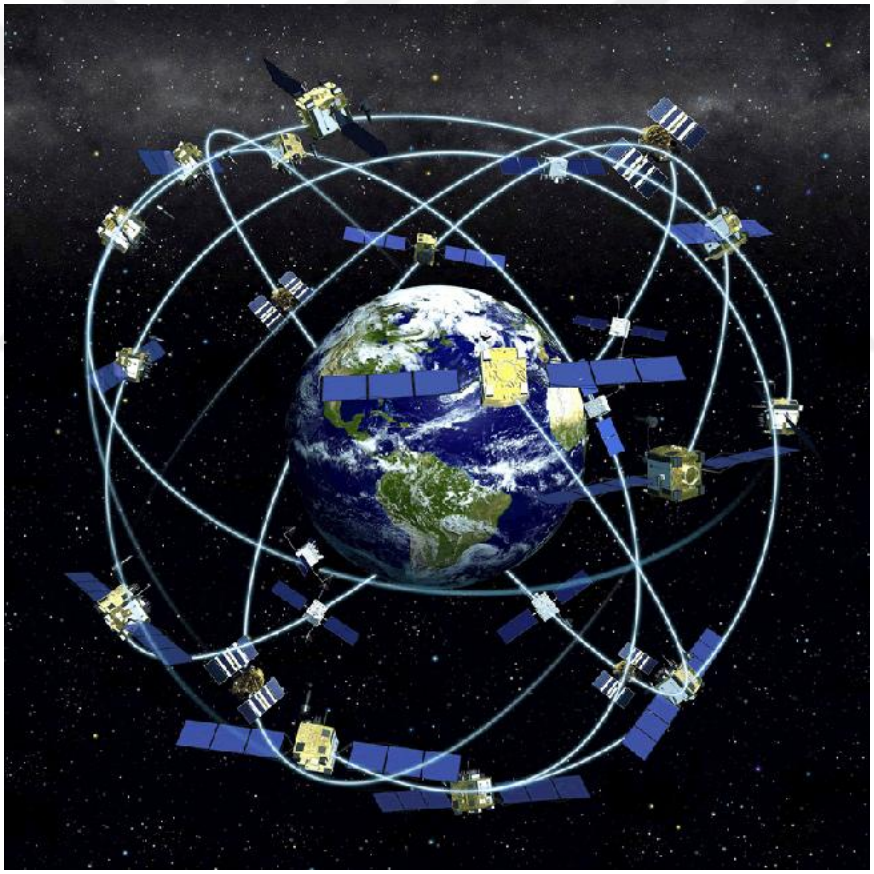
Ticari: Altyapı izleme, ürün teslimatı ve hava görüntüleme gibi uygulamalar için kullanılır.

Hükümet ve Güvenlik Güçleri: İtfaiye ve devriye gibi uygulamalar için kullanılır.

Askeri: Gözetleme ve savaş saldırıları gibi uygulamalar için kullanılır.

3. GLOBAL POSITIONING SYSTEM (GPS)

Global Positioning System (GPS), başlangıçta yalnızca askeri kullanım amacıyla geliştirilen, günümüzde ise küresel ölçekte hem askeri hem de sivil uygulamalarda vazgeçilmez hale gelen bir uydu tabanlı konum belirleme sistemidir. GPS'in temelleri, 1950'li yıllarda ABD tarafından yürütülen erken dönem konumlama projelerine dayanmaktadır. Bu dönemde, ABD ordusu tarafından düşük Dünya yörüngesine (LEO) yerleştirilen altı adet uydu ile, 150 ve 400 MHz frekans aralıklarında çalışan deneysel bir sistem geliştirilmiş ve bu sistem aracılığıyla ilk konum verileri elde edilmiştir [9]. Bu erken uygulamalarla elde edilen konum doğruluğu, tek taşıyıcı frekans kullanıldığında yaklaşık 100 metre, çift taşıyıcı frekansla birlikte kullanıldığında ise 20 m doğrulukla konum tespiti yapabiliyordu. Şekil 3.1'de görüldüğü gibi GPS sistemi uyduları dünyamızın çevresinde yörüngelerinde konumlanmıştır.



Şekil 3.1. GPS Sistemi

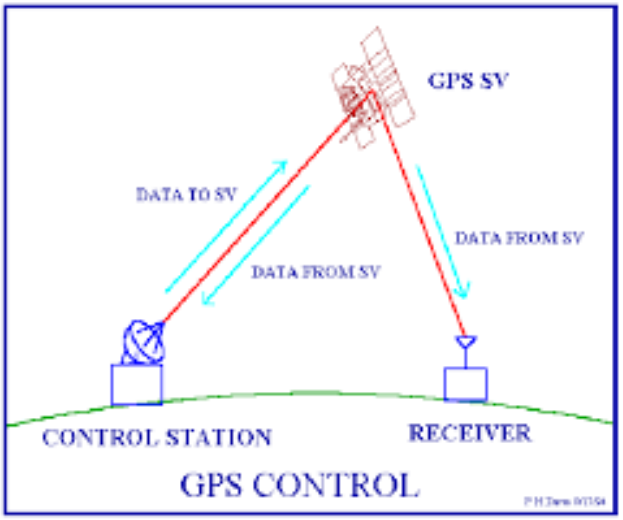
GPS sisteminin günümüzdeki hâliyle temellendirildiği NAVSTAR (Navigation System with Timing and Ranging) programı kapsamında, 24 uydudan oluşan bir uydu takımyıldızı planlanmıştır. Bu sistem, 21 adet aktif (asil) ve 3 adet yedek uyduyu kapsayan bir yapıda tasarlanmış ve ilk GPS uydusu 1978 yılında uzaya fırlatılmıştır. 1994 yılına gelindiğinde ise tüm sistem tamamlanarak **tam operasyonel kapasiteye** ulaşmıştır [10]. Bu uydular, yaklaşık 20.200 kilometre yükseklikte bulunan **Orta Dünya Yörüngesine (MEO)** konuşlandırılmıştır ve Blok I, Blok II ve Blok III olmak üzere farklı

teknoloji seviyelerine sahip üç ana sınıfta toplanmıştır. Her bir blok, belirli bir dönemin teknolojik kapasitesini yansıtmakta ve sistemin zaman içinde güncellenmesini sağlamaktadır.

Başlangıçta 24 uyduyla sınırlandırılan sistem, zamanla artan konumlama talepleri, daha yüksek hassasiyet beklentileri ve teknolojik ilerlemeler doğrultusunda genişletilmiş ve modernize edilmiştir. Özellikle **Blok III** uydularının devreye girmesiyle birlikte, sistemin performansı ciddi ölçüde artırılmıştır. Günümüzde, yörüngede aktif durumda bulunan **31 GPS uydusu**, altı ayrı yörüngede eşit olarak dağıtılmış biçimde faaliyet göstermektedir. Bu genişletme sayesinde, kullanıcılar dünya üzerinde herhangi bir noktada aynı anda birden fazla uydu sinyali alabilmekte ve bu da konumlama doğruluğunu artırmaktadır [10].

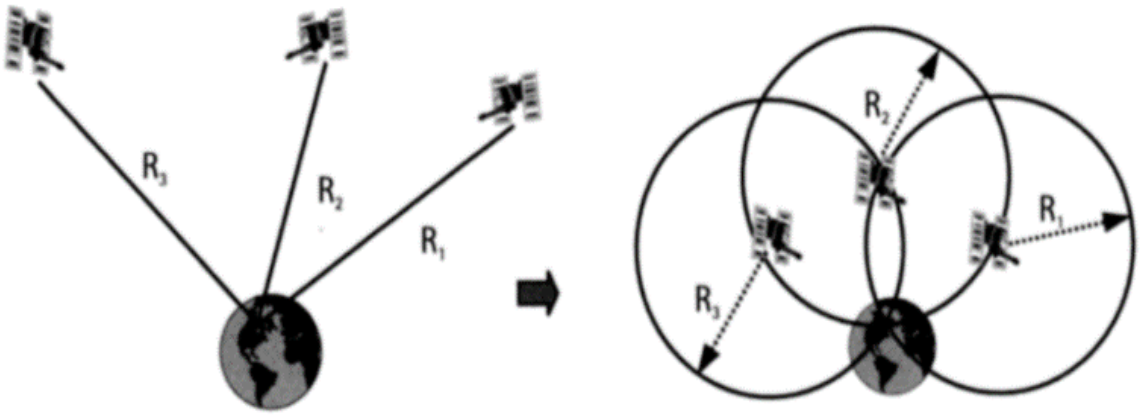
Taşıyıcı frekans sayısındaki artış, sistemin konumlama hassasiyetini daha da geliştirmiştir. Başlangıçta sadece **L1 (1575.42 MHz)** frekans bandı kullanılırken, daha sonra **L2 (1227.60 MHz)**, **L3 (1381.05 MHz)**, **L4 (1379.91 MHz)** ve **L5 (1176.45 MHz)** frekansları da sisteme eklenmiştir. Bu frekansların her biri farklı operasyonel ihtiyaçlara hizmet etmektedir. **L3**, nükleer patlama tespiti gibi askeri amaçlara yönelik sinyaller taşırken, **L4**, iyonosferik düzeltme çalışmaları için geliştirilmiştir. **L5** ise yüksek hassasiyet gerektiren sivil uygulamalarda (örneğin havacılıkta) kullanılmak üzere geliştirilmiştir [11].

Her bir GPS uydusu, taşıyıcı sinyalin yanı sıra iki tür kod (C/A ve P(Y)) ve bir navigasyon mesajı içerir. Bu sinyaller **L bandında** yayınlanmakta ve kullanıcı alıcısında işlenerek kesin konum, hız ve zaman bilgisi elde edilmektedir. Uydular aynı zamanda **Doppler etkisi** ile hareket bilgisi sağlamakta, bu sayede daha hassas dinamik konum hesaplamalarına olanak tanımaktadır. Son yıllarda geliştirilen algoritmalar ve yüksek doğruluklu saat sistemleri ile GPS sisteminin konumlama hatası 5 metre altına indirilmiştir. Özellikle **diferansiyel GPS (DGPS)**, **gerçek zamanlı kinematik (RTK)** ve **yardımlı GPS (A-GPS)** gibi tekniklerin entegrasyonu ile bu doğruluk daha da artırılmıştır [11].



Şekil 3.2. GPS Çalışma Mantığı

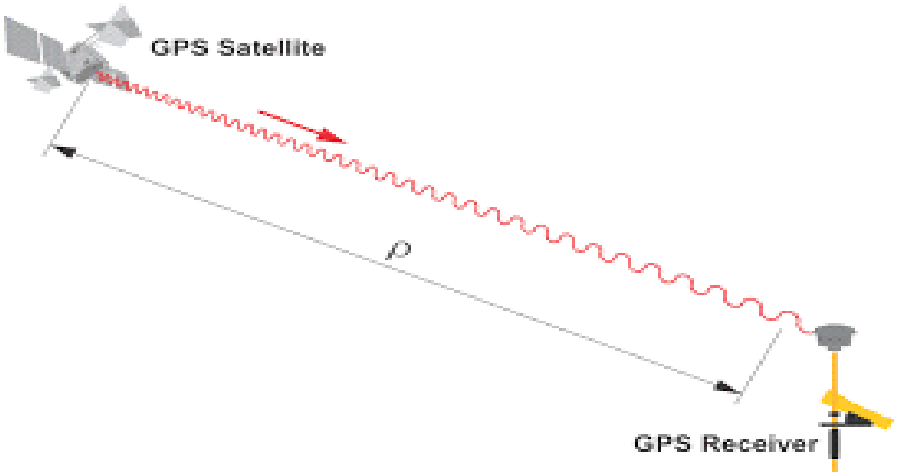
Sonuç olarak, GPS sisteminin tarihsel gelişimi yalnızca teknolojik bir ilerleme değil, aynı zamanda modern savunma ve sivil altyapılar için kritik bir dönüşümün parçası olmuştur. Bugün hem askeri operasyonlarda yüksek hassasiyetli yönlendirme sistemleri için hem de sivil kullanımda ulaşım, haritalama, mobil cihaz konumlaması, tarım ve lojistik gibi sayısız uygulamada temel bileşenlerden biri olarak hizmet vermektedir. GPS sisteminin temel yaklaşımı Şekil 3.3.'de gösterilmiştir.



Şekil 3.3. GPS Sisteminin Temel Yaklaşımı

3.1. GPS Sinyalinin Yapısı

GPS (Global Positioning System) uyduları, sürekli olarak Dünya'ya yönlendirilmiş biçimde elektromanyetik dalgalar aracılığıyla bilgi içeren mikrodalga sinyalleri yaymaktadır. Bu sinyaller, birer **taşıyıcı frekans**, **dijital kod** ve **navigasyon mesajı** içerir. GPS alıcıları, bu bileşenleri çözümleyerek konum, hız ve zaman bilgilerini hesaplar. Her bir GPS sinyali, belirli taşıyıcı frekanslar üzerine yerleştirilen özel kodlama teknikleriyle yapılandırılmıştır. GPS sinyalinin yapısı Şekil 3.4'de gösterilmiştir.



Şekil 3.4. GPS Sinyalinin Yapısı

GPS sisteminde **L1 frekansı**: 1575.42 MHz **L2 frekansı**: 1227.60 MHz olmak üzere iki ana taşıyıcı frekans kullanılmaktadır. Bu frekansların elektromanyetik dalga boyları, sırasıyla yaklaşık **19 cm (L1)** ve **24.4 cm (L2)** olarak hesaplanır. Bu dalga boyu değerleri, elektromanyetik dalganın frekansı (f) ile ışık hızı (c) arasındaki $\lambda = \frac{c}{f}$ ilişkisiyle belirlenmektedir [12]. Sinyallerin mikrodalga aralığında olması, iyonosfer ve troposfer gibi atmosfer katmanlarında sınırlı ama ölçülebilir derecede sapma ve gecikmeye maruz kalmasına neden olmaktadır.

İki taşıyıcı frekansın bir arada kullanılması, özellikle **iyonosferik gecikme hatalarının** düzeltilmesine olanak tanır. Bu gecikmeler, sinyallerin atmosfer içinden geçerken karşılaştığı yoğunluk farklılıklarından kaynaklanır ve tek frekans kullanan sistemlerde doğruluk kayıplarına yol açabilir. Çift frekanslı GPS alıcıları, L1 ve L2 sinyallerini karşılaştırarak bu sapmayı matematiksel olarak hesaplayabilir ve böylece daha hassas konum verileri elde edebilir [13].

Her GPS uydusu aynı L1 ve L2 taşıyıcı frekanslarını kullanmasına rağmen, sinyallerin karışmaması ve alıcı tarafından ayırt edilebilmesi için farklı **kod modülasyonları** uygulanır. Bu yöntem, sinyal parazitini ve girişimini azaltmakla kalmaz, aynı zamanda her uydunun alıcı tarafından tanınmasını da sağlar. GPS sinyal kodları genel olarak iki ana kategoriye ayrılır:

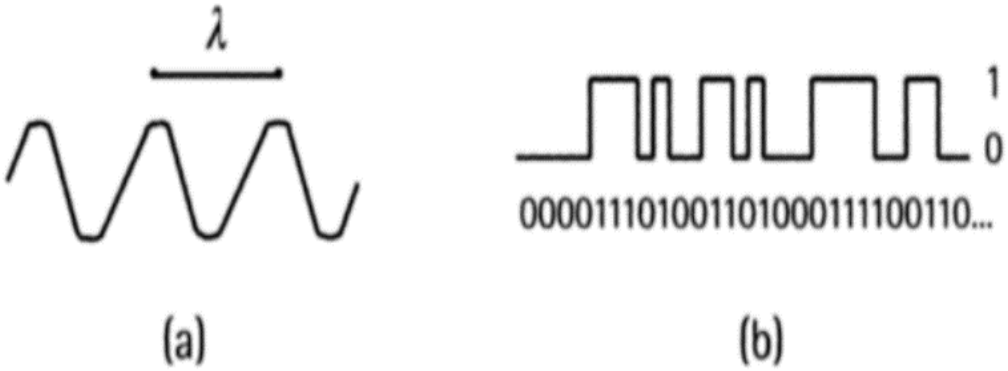
C/A Kodu (Coarse/Acquisition Code): Daha yaygın olarak bilinen ve sivil kullanıcılar için tasarlanmış bir "kaba yakalama kodudur". Yalnızca L1 taşıyıcı frekansı üzerine modüle edilir ve 1.023 MHz hızında yayımlanır.

P Kodu (Precise Code): Daha karmaşık ve daha uzun bir diziye sahip olan, askeri kullanıma özel "hassas kod" olarak adlandırılır. P-kodu hem L1 hem de L2 frekansları üzerine modüle edilir ve 10.23 MHz hızında çalışır [14].

P-kodunun şifrelenmiş versiyonu olan **Y-kodu**, yalnızca askeri yetkili alıcılar tarafından çözülebilecek biçimde kriptolanmıştır ve **anti-spoofing** amacıyla kullanılır. Bu yapı, düşman unsurların GPS sinyallerini taklit ederek yanıltıcı bilgiler göndermesini (spoofing) önlemeye yardımcı olur. C/A ve P kodlarının birlikte kullanılması, sivil ve askeri kullanıcılar arasında **farklı hassasiyet seviyeleriyle hizmet sunulmasına** olanak sağlar.

Her sinyal aynı zamanda bir **navigasyon mesajı** taşır. Bu mesaj, uydunun yörünge parametreleri (efemeris verisi), saat düzeltmeleri ve takımyıldızın genel durumu hakkında bilgi içerir. Navigasyon mesajı, 50 bps (bit per second) hızla iletilen ve genellikle bir GPS alıcısının uydunun pozisyonunu ve zamanlamasını doğru şekilde çözümlemesi için gereken temel bilgileri sağlar.

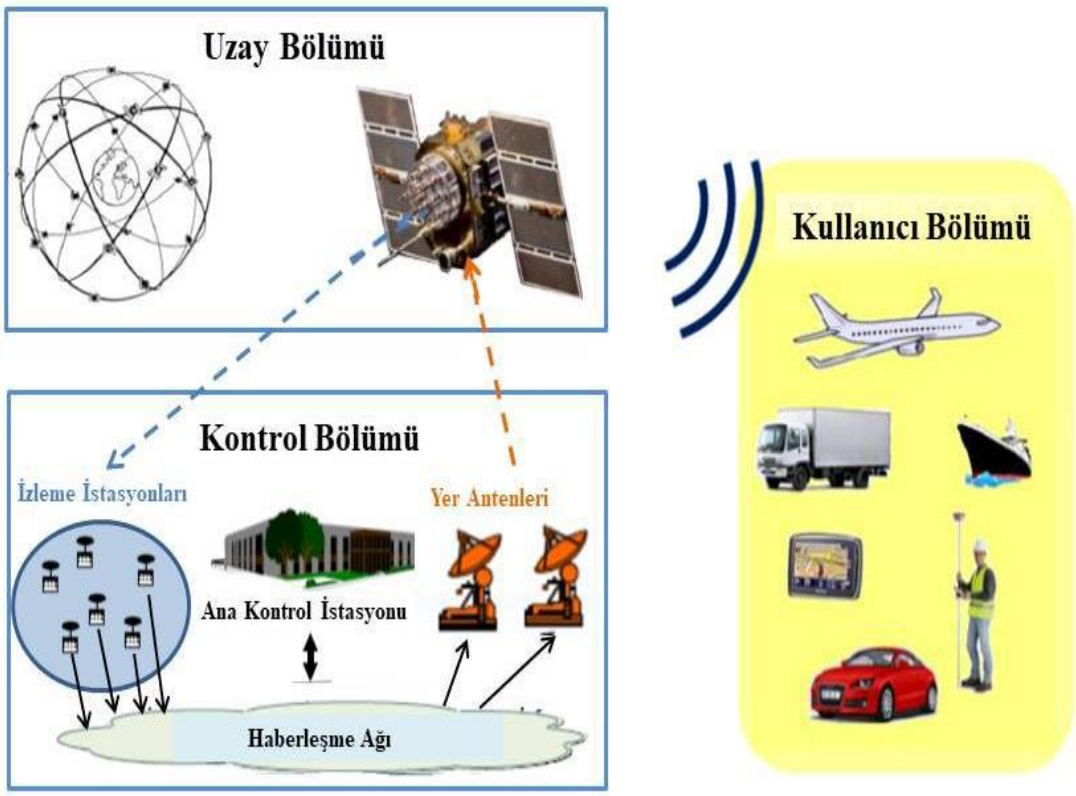
GPS sinyal yapısı; elektromanyetik spektrum, modülasyon teknikleri, kodlama sistemleri ve navigasyon verilerinin hassas şekilde senkronize edilmesini içeren oldukça sofistike bir sistemdir. Bu yapı, GPS alıcılarının dünya üzerinde yüksek doğrulukla konum tespit etmesini ve gerçek zamanlı uygulamalarda etkili performans sergilemesini mümkün kılmaktadır. Sinusoidal Frekans ve Dijital Kod Şekil 3.5'de gösterilmiştir.



Şekil 3.5. Sinusoidal Frekans ve Dijital Kod

3.2. GPS Ana Bölümleri

GPS (Global Positioning System), küresel konum belirleme hizmeti sunmak amacıyla entegre edilmiş üç ana bileşenden oluşur: **Uzay Bölümü**, **Kontrol Bölümü** ve **Kullanıcı Bölümü**. Bu üç bölüm, sistemin bütüncül ve kesintisiz şekilde çalışmasını sağlar. Şekil 3.6'da gösterilen bu yapı, GPS ana bölümlerini oluşturmaktadır.



Şekil 3.6. GPS Ana Bölümleri

Uzay bölümü, sistemin çekirdeğini oluşturan ve Dünya çevresindeki yörüngelere yerleştirilmiş GPS uydularından meydana gelir. Bu uyduların temel görevi, belirli taşıyıcı frekanslar üzerinden kullanıcıya sürekli olarak navigasyon sinyalleri iletmektir. Tam küresel kapsama sağlamak üzere en az **24 operasyonel uydu** planlanmış olup, günümüzde bu sayı **31'e çıkarılmıştır** [15]. Uydular, yaklaşık **20.200 km yüksekliğe sahip orta Dünya yörüngelerinde (MEO)** hareket eder ve her biri **11 saat 58 dakikada Dünya etrafında bir turunu tamamlar**.

GPS uyduları, eşit aralıklarla yerleştirilmiş **6 farklı yörünge düzlemi** üzerinde ve her düzlemde **4 uydu** olacak şekilde konumlandırılmıştır. Bu yapılandırma sayesinde, Dünya üzerindeki herhangi bir noktadan en az 4 farklı GPS uydusunun eş zamanlı olarak gözlemlenmesi garanti altına alınmaktadır. Bu minimum 4 uydu sinyali, 3 boyutlu konumlama (x, y, z) ve zaman eşlemesi için yeterlidir.

GPS uyduları farklı nesillerde üretilmiş ve teknolojik ilerlemelere bağlı olarak çeşitli iyileştirmelerle donatılmıştır. Bugüne kadar geliştirilen GPS uyduları **Legacy Uydular**: Block I, Block II, Block IIA, **Modernize Uydular**: Block IIR-M, Block IIF, GPS III ve yeni nesil **GPS IIIF** olmak üzere yedi nesilden oluşmaktadır.

Bu nesiller arasındaki farklar; sinyal gücü, frekans kapasitesi, sinyal güvenliği, atomik saat hassasiyeti ve hizmet ömrü gibi teknik kriterlerle belirlenmektedir.

Her GPS uydusu, **PRN (Pseudo Random Noise) numarası**, **SVN (Space Vehicle Number)**, **Yörünge düzlemi ve pozisyon bilgisi** gibi çeşitli yöntemlerle tanımlanabilir.

Bunlar arasında özellikle **PRN kod numaraları**, alıcıların uyduları tanımlamasında en yaygın kullanılan yöntemdir. Bu kodlar sayesinde her uydu, alıcı cihazlar tarafından ayırt edilebilir ve ilgili navigasyon verileri doğru şekilde çözümlenebilir [15].

Kontrol bölümü, GPS sisteminin işlevselliğini ve sürekliliğini sağlamakla görevli olan yer tabanlı birimlerden oluşur. Bu bölüm; **Ana kontrol istasyonu**, **İzleme (monitoring) istasyonları** ve **Yer antenleri** olmak üzere üç alt birimden meydana gelir.

Ana kontrol istasyonu, GPS sisteminin merkezi yönetim noktasıdır. Sistem üzerindeki tüm uyduların konumları, sağlık durumları ve yörüngesel parametreleri bu merkezde sürekli olarak takip edilir ve gerekli düzeltmeler yapılır. Uyduların hassas efemeris verileri, saat düzeltmeleri ve navigasyon mesajları bu merkezden hazırlanır ve uygun sinyallerle uydulara iletilir.

İzleme istasyonları, Dünya'nın çeşitli noktalarına konumlandırılmış olup, GPS uydularının gönderdiği sinyalleri izleyerek veri toplarlar. Bu veriler; Navigasyon sinyalleri, Atmosferik gecikme verileri, Taşıyıcı frekans ölçümleri, Uydu saatleri gibi bilgilerden oluşur. İzleme istasyonları bu verileri ana kontrol istasyonuna ileterek sistemin doğrulukla çalışmasına katkıda bulunurlar.

Yer antenleri ise, ana kontrol istasyonu tarafından oluşturulan telemetri ve komut verilerini uydulara göndermekle görevlidir. Aynı zamanda uydulardan alınan verileri de toplar. Bu iletişim, genellikle **S bandı** üzerinden gerçekleşir. Yer antenleri, hem yukarı (uplink) hem de aşağı (downlink) bağlantılar için kritik öneme sahiptir [16].

Kullanıcı bölümü, GPS sisteminin en geniş bileşenidir ve hem **askeri** hem de **sivil kullanıcıları** kapsar. GPS sinyallerini alabilen tüm cihazlar bu segmentin bir parçasıdır. Kullanıcılar, GPS uydularından gelen sinyalleri işleyerek **konum (latitude, longitude, altitude)**, **hız**, **yön** ve **zaman** bilgilerine ulaşabilirler. Bu bilgiler, navigasyon, haritalama, zaman senkronizasyonu, ulaşım, tarım, havacılık ve afet yönetimi gibi birçok farklı alanda kullanılmaktadır [17].

Modern GPS alıcıları; otomobillerde, cep telefonlarında, İHA'larda, gemilerde, trenlerde ve kişisel cihazlarda yaygın biçimde bulunmaktadır. Ayrıca, gelişmiş kullanıcı segmenti uygulamaları, **diferansiyel GPS (DGPS)**, **RTK (Real-Time Kinematic)** ve **GNSS destekli hibrit sistemler** gibi teknolojileri kullanarak çok daha yüksek doğrulukla konumlama sağlamaktadır.

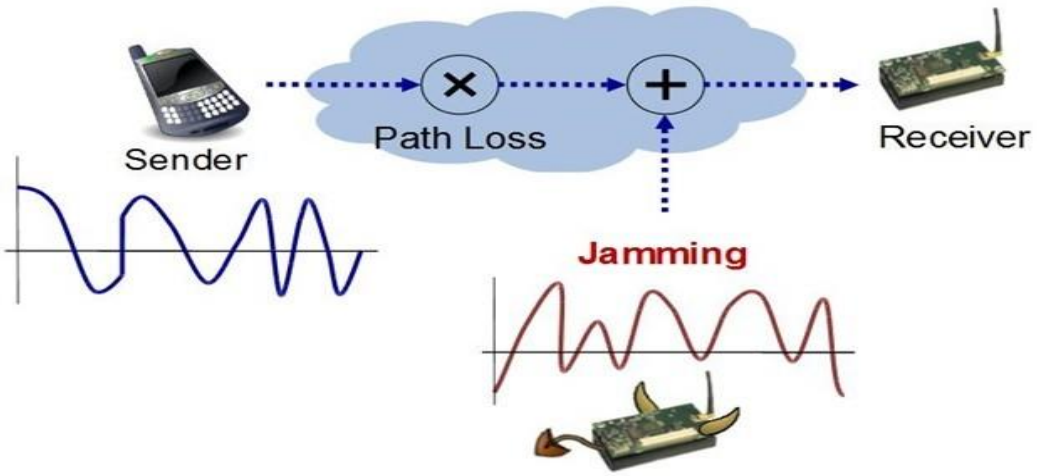
4. GPS KARIŞTIRMASI

İşletim moduna bağlı olarak (manuel, tam ve kısmen otonom), farklı durumlar nötralizasyon için farklı yaklaşımları gerektirir. Bir manuel veya yarı-otonom İHA için, yer istasyonu ve İHA arasındaki RF radyo iletişimi çeşitli protokoller üzerinden sabit paket yapısı ile gerçekleşir. Bu paketler ele geçirilip çözümlenerek paket mimarisi elde edilebilir ve böylece bir aldatma saldırısı başlatılabilir. Büyük miktarda enerji iletimi gerçekleştiren RF engelleyiciler de iletişimi bozmak için kullanılabilir. Bu, İHA'nın başarısız güvenlik önlemlerini etkinleştirmesine neden olabilir, bu güvenli bir iniş yapmak, belirlenen bir baz konumuna dönmek veya rastgele uçarak çarpma olabilir. Otonom bir İHA için, sensör değerleri bozulabilir. Özellikle GNSS sinyalleri engellenebilir ve aldatılabilir. Bunların yanı sıra, mümkün olan diğer bazı fiziksel saldırılar da vardır [18].

4.1. Karıştırma (Jamming)

İHA ve yer kontrolü arasındaki RF radyo iletişiminde, RF engelleme teknikleri, gürültü müdahalesi seviyesini artırmak için kullanılır. Bu, alıcının SNR'sini azaltır. Bunun sonucunda, alıcının göndericiden gelen komutlara cevap vermesini engeller ve böylece işleyişini etkisiz hale getirir. Bu nedenle, pilot veya uydu sistemlerinden gelen sinyaller, bunlara bağlı manuel ve otonom İHA'ların işleyişini bozmak için engellenebilir. Bununla birlikte, yalnızca IMU'lar ve kameralar gibi diğer sensörleri kullanarak çalışan bazı İHA'lar, bu engelleme tekniğine karşı koyabilir [19].

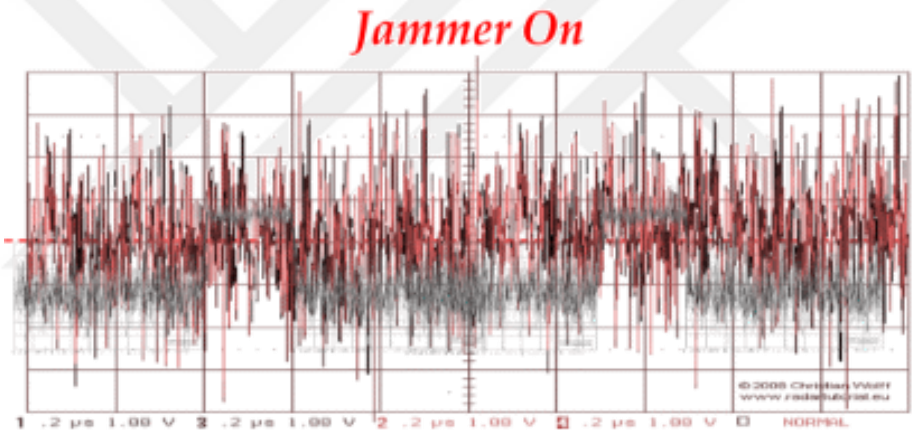
Farklı İHA'lar farklı yayılma spektrumu ve modülasyon teknikleri kullanabilir. Engelleme etkinliğini azaltmak için, çeşitli yöntemler ayrıca yazılım tanımlı ağlara dayalı olarak geliştirilmiştir. Bu nedenle, bu duruma bağlı olarak, RF alıcısında müdahaleyi etkin bir şekilde tanıtmak için farklı RF engelleme tekniklerinin daha verimli olacağı farklı RF engelleme teknikleri mevcuttur [20]. Örnek bir jamming çalışması şekil 4.1 ‘de gösterilmiştir.



Şekil 4.1. Jamming

4.1.1. Noise Jamming

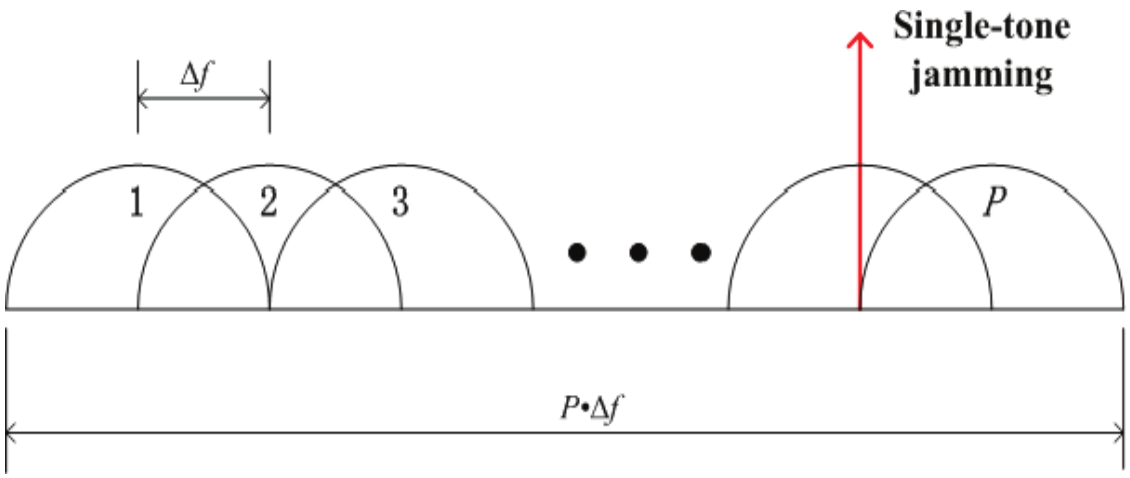
Bir diğer adı Barrage Engelleme olan, geniş bant modüle edilmiş sinyalin küçük bir kısmına veya tamamına gürültü sinyali uygulanan en basit engelleme şeklidir. Bu tür engelleme doğrudan sistemin kanal kapasitesini etkiler ve azaltır. Alıcıda SNR değerini azaltır, böylece kanal kapasitesini azaltır ve bilgi hata oranını artırır. Gürültü engelleme, her iletim arasında gönderici ve alıcı arasında gereken saat senkronizasyonu ve takip sırasında arka plan müdahalesi ekleyerek özellikle FHSS sistemlerini etkiler. Sentetik Açıklıklı Radar (SAR), iki boyutlu ve üç boyutlu mekânsal haritalama için kullanılan özel bir radardır ve genellikle Simultaneous Localization and Mapping (SLAM) gibi yöntemler kullanılarak İHA'larda otonomi sağlamak için kullanılır. Gürültü engelleme, SAR sistemini işe yaramaz hale getirmek için yeterli olan radyo müdahalesi üretir, böylece yansımaları gizler [21]. Şekil 4.2'de de görüldüğü üzere noise jamming tüm sinyali karıştırmıştır.



Şekil 4.2. Noise Jamming

4.1.2. Tone Jamming

Bu tür engellemede, spektrumdaki bir veya daha fazla ton stratejik olarak engellenir ve müdahaleyi tanıtmak için kullanılır. Engelleme performansı, tonların spektrum içindeki konumuna ve iletim gücüne bağlıdır. İletim gücü, ton üzerindeki müdahaleyle doğru orantılıdır. Bu teknik, engelleme marjını aşmak için yeterli müdahale oluşturabilme yeteneğine bağlıdır, bu da çok sayıda ton hedeflendiğinde büyük güç gerektirir. Ton engelleme tek bir ton üzerinde (monoton) ya da birden çok ton üzerinde (çok tonlu) olmak üzere iki şekilde olabilir. Monoton engelleme zayıf performans sergiler, çünkü bir kanalın eksik olması sistem genel performansını etkilemez. Hatta çok tonlu engellemede bile, önemli ölçüde müdahale tanıtabilmek için düşmanın spektrumdaki yeterli sayıda kanalı engellemesi gerekir [22]. Belirli tonlarda yapılan tone jamming örneği şekil 4.3'te gösterilmiştir.

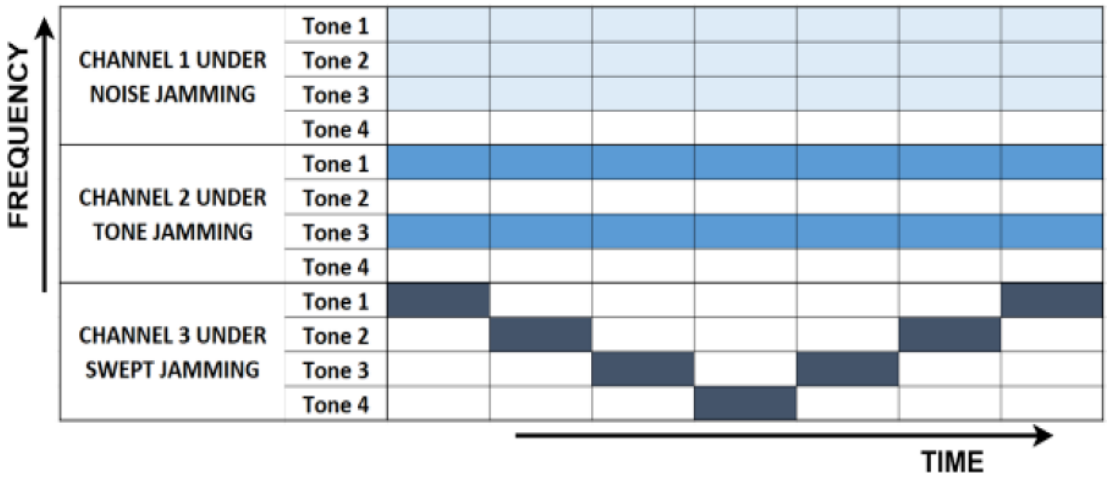


Şekil 4.3. Tone Jamming

4.1.3. Swept Jamming

Süpürme engellemesinde, ilgili frekans spektrumu boyunca tarama yapılır. Belirli bir an için, yalnızca tek bir frekans hedeflenir. Ancak, zaman içinde, engelleyici hedef frekansı süpürerek bir dizi frekans bandını kapsar. Bu nedenle, uygulamasında gürültü ve ton engelleme bir karışımıdır. Gürültü engelleme ile benzer şekilde, tek bir tona odaklanır, ancak süpürerek, aynı zamanda ton engelleme de taklit edilir. Gürültü veya ton engelleme gibi, süpürme engelleme dalgası, veri sinyalinin tüm spektrumunda bulunan tüm atlama frekanslarını kapsadığından emin olur [23].

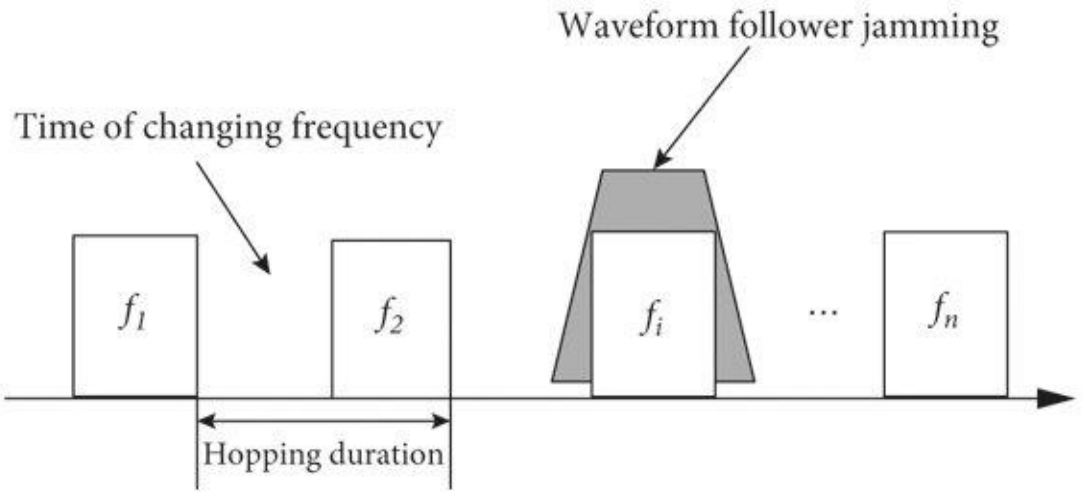
Süpürme engelleme, veri frekans bantlarının, frekans bantlarının periyodik olarak yarı rastgele bir şekilde atlama yaptığı sistemlerin aksine, sabit olduğu sistemlere karşı iyi performans gösterir. Süpürme engelleme, GPS sinyallerinin zayıf gücünden dolayı genellikle GPS destekli sistemlere karşı kullanılır. GNSS'yi süpürme engellemeye karşı korumanın yolları da sürekli olarak aktif bir şekilde geliştirilmekte ve analiz edilmektedir [24]. Noise, tone ve swept jamming ile ilgili grafik Şekil 4.4'te verilmiştir.



Şekil 4.4. Noise, Tone ve Swept Jamming

4.1.4. Follower Jamming

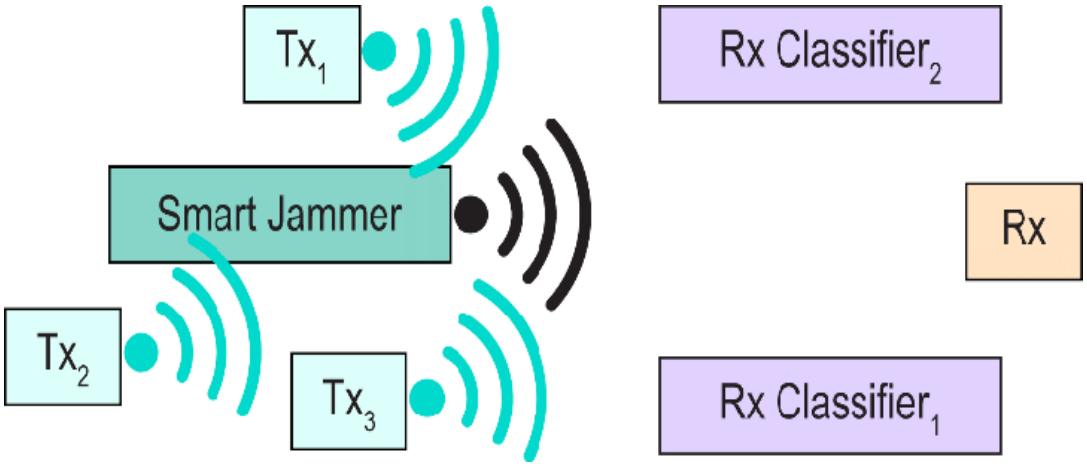
Takipçi engelleyici her zaman bir sistemin gittiği yeni frekans atlama noktasını bulmaya çalışır ve ardından hedef sinyali belirler. Doğrulandıktan sonra, bulunan frekansı engellemeye çalışır. Hedef sistemin frekansını bulmak için, engelleyicinin spektrumda enerji kayıplarını ve kazançlarını ölçmesi gerekir. Spektrumda enerji kazancı, yeni bir sinyalin girdiğini gösterirken, enerji kaybı bir sinyalin banttan çıktığını gösterir. Ancak, hedef sinyalin belirli bir enerji değişikliğine karşılık gelip gelmediğini doğru bir şekilde belirlemek önemlidir, bunun için analiz yapılması gerekir [25]. Follower jamming ile ilgili örnek şekil 4.5'te verilmiştir.



Şekil 4.5. Follower Jamming

4.1.5. Smart Jamming

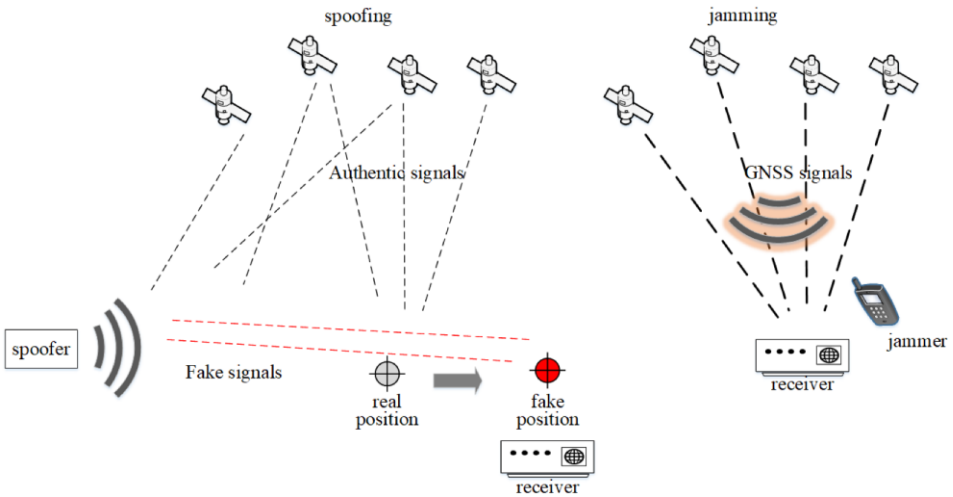
Bu tür engelleme, Radyo Frekansı Entegre Devre (RFIC) özellikleri gibi kaynaklardan önceden bilinen hedef sinyal özellikleri olduğunda uygulanabilir. Akıllı engellemede, başarılı iletişimi engellemek için yalnızca gerekli sinyallere saldırılır ve bu nedenle güç verimli ve etkilidir. Bunun sağlanması için iletilen verilerin analiz edilerek kritik noktaların belirlenmesi gerekmektedir. Yazılım Tanımlı Radyolar kullanılarak protokol bilinci olan engelleme teknikleri geliştirilebilir. Hedef sinyal analiz edildikten sonra, benzeri tarama desenleri (FHSS sistemleri), PN kod veri hızı (DSSS sistemleri) ve modülasyon teknikleri gibi özellikler açısından benzer bir engelleme sinyali üretilebilir. Bu tür sistemlerin uygulanmasına ilişkin literatür, sistemde tanıtılan hata oranı (BER) açısından diğer engelleme tekniklerine kıyasla enerji verimli engelleme performansını sunmaktadır. Hedef sinyalleri başarılı bir şekilde engellemede diğer teknikleri geride bıraktığı, ancak hedef sinyalin analizine dayandığı bulunmuştur [26]. Şekil 4.6'da smart jamming ile ilgili örnek verilmiştir.



Şekil 4.6. Smart Jamming

4.1.6. GNSS Jamming

Günümüzde neredeyse tüm İHA uygulamaları bir otomatik pilot işlevselliği içerir. Çalışma modları kısmen veya tamamen otonomdur. İHA'nın mevcut özelliklerini, yönelimi, konumu ve ivmesi gibi tahmin etmek için birçok sensör ve yerleşik donanım bulundururlar. Bunlardan biri, konumlandırma için sinyaller sağlayan GPS gibi bir GNSS modülüdür. GPS sinyalleri, zayıf sinyal gücü nedeniyle genellikle savunmasızdır ve gürültü ile dış müdahalelere son derece duyarlıdır. GNSS engelleme uygulaması, bu bağlamda İHA'ları devre dışı bırakmak için bir teknik olarak kullanılmasına rağmen, aynı yöntemlerin navigasyon gibi diğer kritik uygulamalardaki GNSS sistemlerini devre dışı bırakmak için de kullanılabilir olması nedeniyle aktif bir alandır. GPS sinyalleri için farklı engelleme teknikleri, spektral verimlilik, enerji verimliliği ve karmaşıklık temelinde incelenmiş, analiz edilmiş ve değerlendirilmiştir. Buna göre, protokol bilinci olan engelleme veya akıllı engelleme en verimli bulunmuştur. GPS engelleme oldukça yaygındır ve bu tür engelleyiciler kolayca piyasada bulunmaktadır [27]. GNSS jamming ile ilgili örnek şekil 4.7'de verilmiştir.



Şekil 4.7. GNSS Jamming

5. GPS SİNYALLERİ ÜZERİNDE JAMMİNG TÜRLERİNİN UYGULANMASI

GPS (Global Positioning System) ABD tarafından geliştirilen, konum hız ve zaman bilgisi sağlayan uydu bazlı bir navigasyon sistemidir. Bu sistem kapsamında dünya yörüngesinde dönen minimum 24 aktif uydu yer almaktadır. Bu uydulara sürekli olarak elektromanyetik sinyaller gönderilerek konum hesaplanmaları gerçekleştirilir. GPS başlangıçta askeri amaçlı geliştirilen bir projedir daha sonrasında sivil kullanıma da açılmıştır. Fakat her iki kullanım için iki farklı bant frekansı bulunmaktadır. Sivil kullanımlar için L1 olarak adlandırılan 1575.42 MHz'li frekans kullanılmaktadır. Askeri kullanımlar için ise 1227.60 MHz'li L2 olarak adlandırılan L2 adlı frekans kullanılmaktadır.

GPS sinyalleri 3 temel bileşenden oluşur bunlar sırası ile taşıyıcı sinyal, kod ve navigasyon mesajıdır. Taşıyıcı sinyal sürekli dalga biçimindedir ve sinyalin elektromanyetik olarak iletilmesini sağlar. Kod ise PRN (Pseudorandom Noise) kodları ile gelen sinyalin hangi uydudan ve hangi zamandan geldiğini tespit eder. Son olarak Navigasyon mesajı uyduya ait yörünge bilgileri saat düzeltmeleri ve sistem durumu bilgilerini içerir. Bir GPS alıcısı 4 farklı uydudan gelen sinyalleri analiz ederek konum, zaman, enlem, boylam ve yükseklik hesaplamalarını gerçekleştirir. GPS sinyalleri düşük güçlü olduğu için atmosferik bozulmalar ve jamming işlemlerinden kolaylıkla etkilenebilmektedir. Bu sayede manipüle edilmeye açıktır.

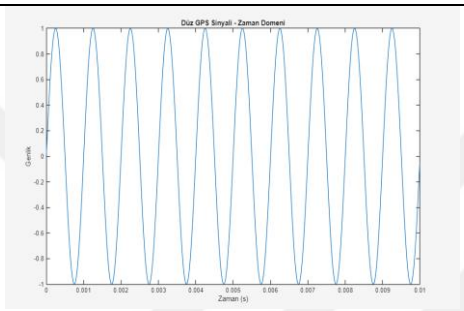
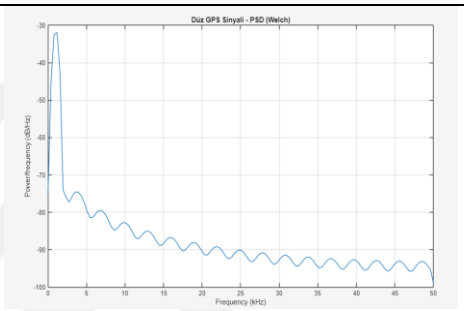
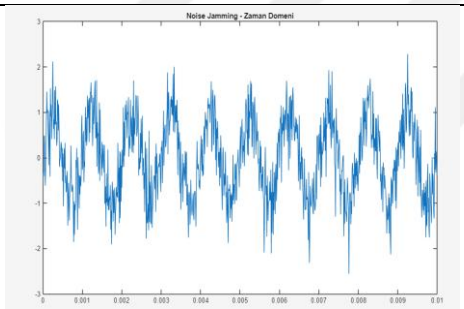
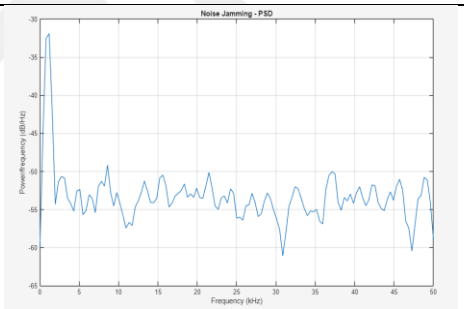
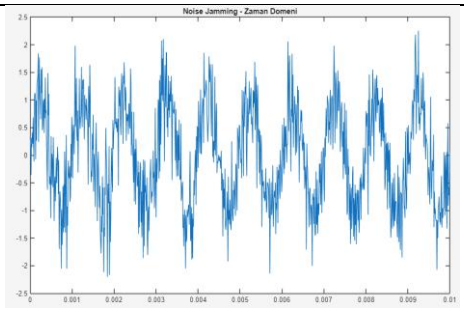
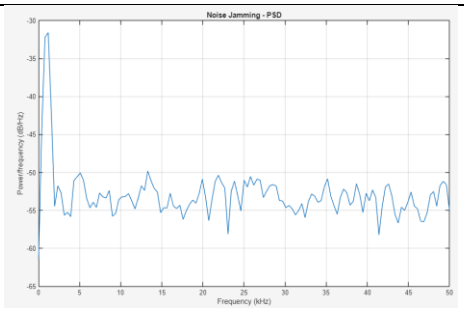
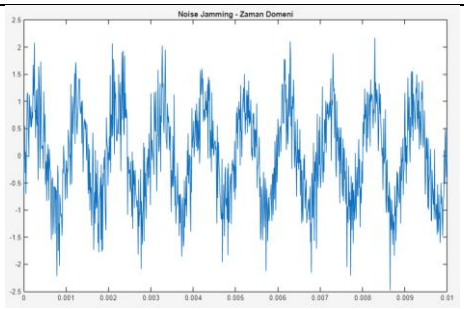
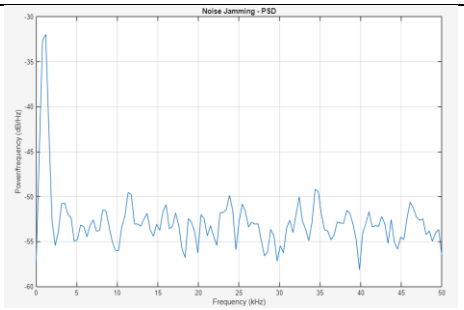
PSD (Güç Spektral Yoğunluğu) bir sinyalin frekans bileşenlerine göre enerji dağılımını tanımlar. Sinyal işleme, haberleşme sistemleri ve elektromanyetik spektrum analizinde yaygın olarak kullanılır. PSD frekans başına düşen ortalama gücü gösterir ve genellikle W/Hz biriminde ifade edilir. Bizde gerçekleştirdiğimiz uygulamaların etkisini ölçmek amacı ile sinyaller üzerindeki PSD durumunu gözlemlemekteyiz. Bu sayede gerçekleştirilen saldırının başarısını daha iyi görebilmekteyiz.

Yapmış olduğumuz simülasyon ortamında 1 kHz'lik taşıyıcı frekans kullanmaktayız. Bu oran gerçek GPS sistemlerinde kullanılan L1 ve L2 bantlarının doğrudan karşılığı değildir fakat L1 bandında akan sivil GPS yapısını modellemek amacıyla sadeleştirilmiştir. Bu sadeleştirme sonucu sinyaller üzerinde gerçekleştirilen analiz işlemleri ve sinyal işleme uygulamaları daha pratik ve anlaşılır bir hale getirilmiştir. Ayrıca her jamming türünde uygun bir artış değeri yakalamak adına özel bir jamming değeri belirlenmiş ve her tür için bu değer arttırılmıştır.

5.1. Noise Jamming İşleminin Farklı Katsayılar İle Birlikte GPS Sinyali Üzerindeki Etkisi

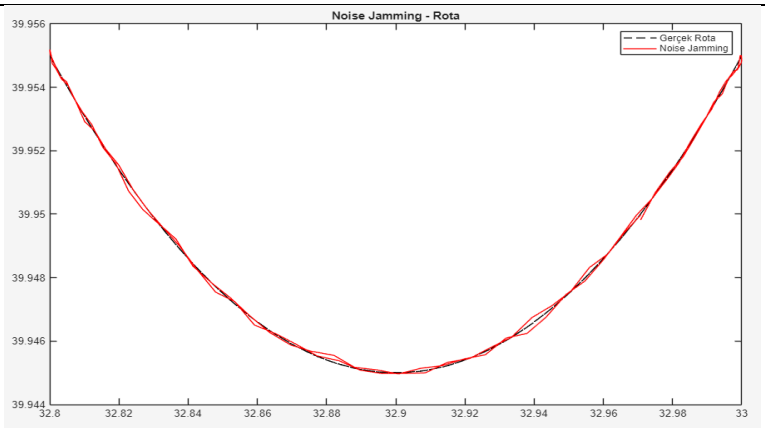
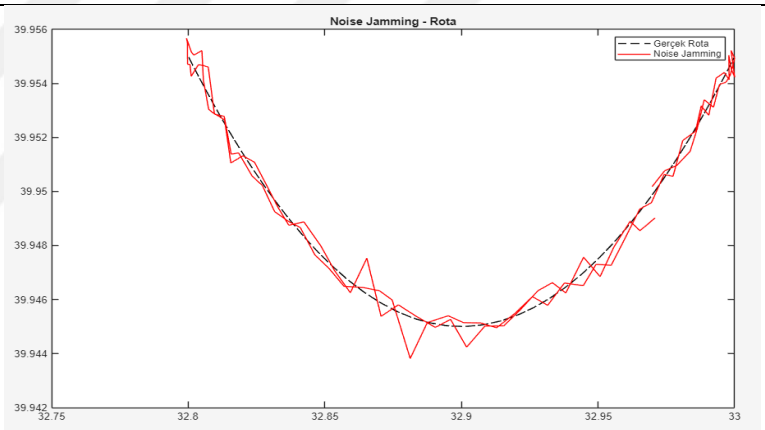
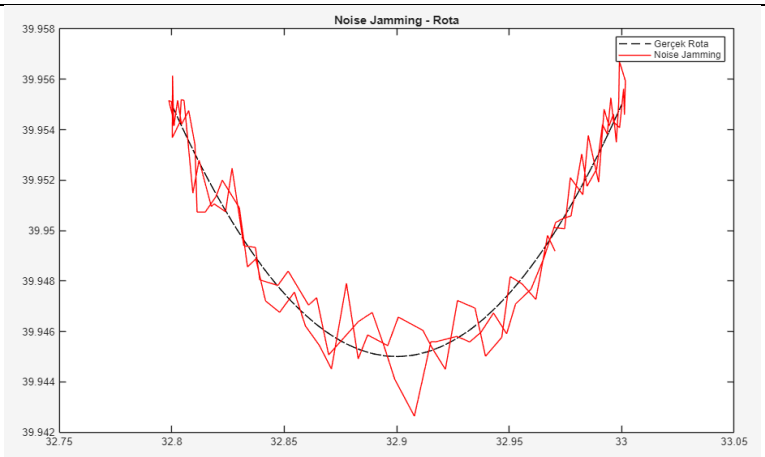
Noise jamming işlemi sinyale geniş bant boyunca parazit uygulamaktadır. Ayrıca konum değerleri rastgele sapma değerleri sayesinde daha komplike bir hale getirilmektedir. PSD verilerinin dalgalı ve gürültülü olmasını sağlar. Bu sayede gelen verinin anlaşılması zorlaştırılır. Tablo 5.1'de PSD analizlerini ve noise jamming işlemi sonrası GPS sinyalinin değişimlerini görüntüleyebilirsiniz.

Tablo 5.1. Noise jamming sonrası GPS sinyali üzerinde gerçekleşen değişiklikler.

Jamming Katsayısı	GPS	PSD
0,0000		
0,0001		
0,0005		
0,0010		

Noise jamming işlemi sonrası GPS sinyallerinde oluşan sapma miktarları ve oluşturulan simülasyona dair konum grafikleri de Tablo 5.2'de gözükmektedir.

Tablo 5.2. Noise jamming sonrası rota üzerinde gerçekleşen değişiklikler.

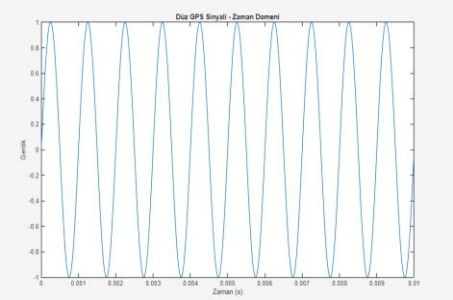
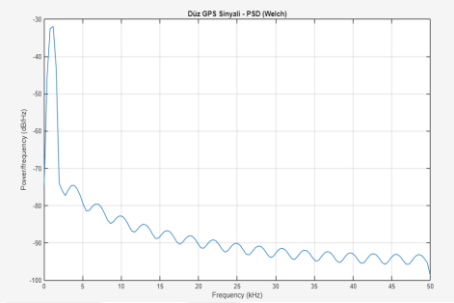
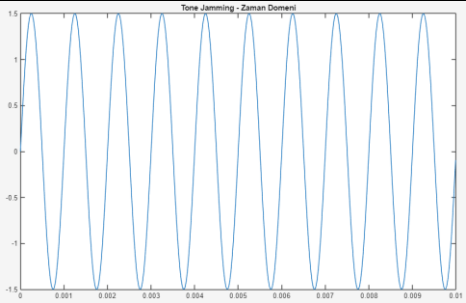
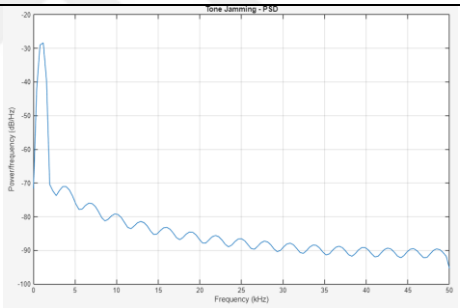
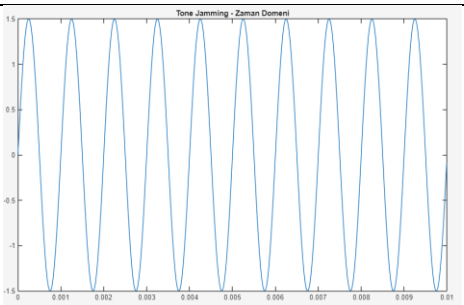
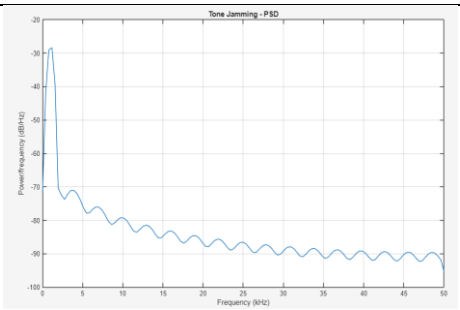
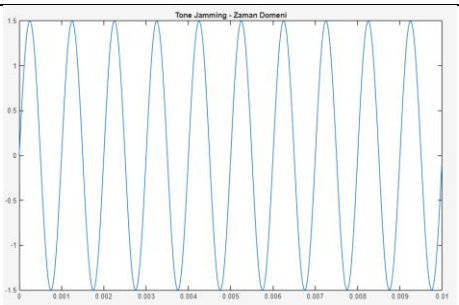
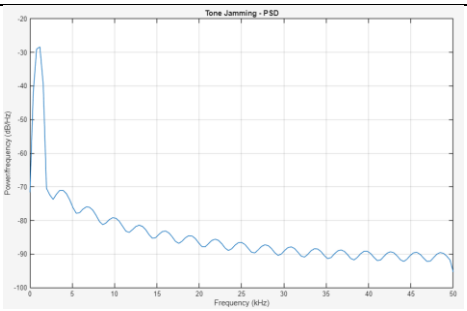
Jamming Katsayısı	**Sapma Miktarı (%)**	**Konum Grafiği**
0,0001	0.04	
0,0005	0.17	
0,0010	0.35	

Noise jamming işlemi sonrasında jamming katsayısı arttıkça tüm sinyaldeki sapma miktarı da artmaktadır. Jamming katsayısı 0,0010 olduğunda gerçek rotadan sapma miktarı % 35'e kadar çıkmaktadır.

5.2. Tone Jamming İşleminin Farklı Katsayılar İle Birlikte GPS Sinyali Üzerindeki Etkisi

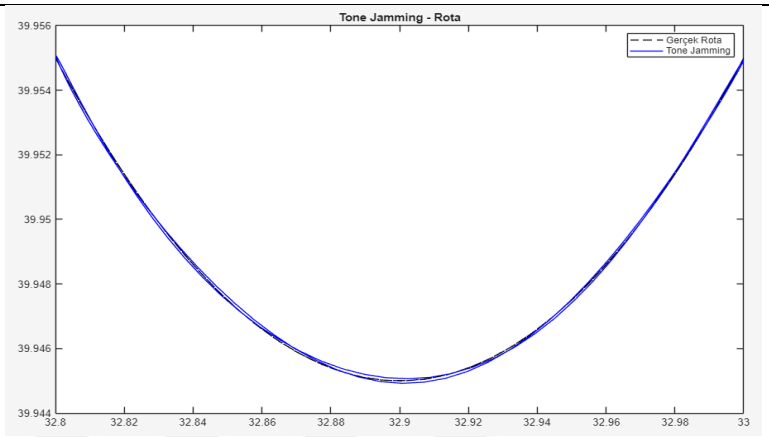
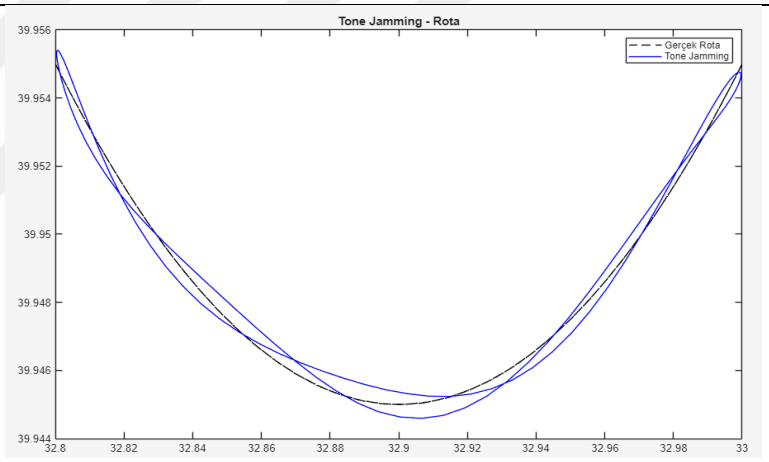
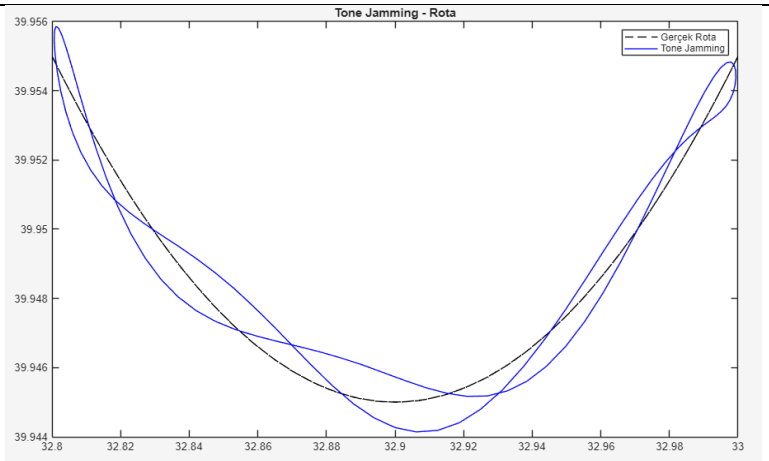
Tone jamming işlemi sabit frekansta sinyal bozmak için uygulamaktadır. Ayrıca saldırının sinyal tipi sabit sinüzoid biçimdedir. Dolayısıyla konum değişikliği sinüs grafiği şeklinde sabit bir sapma göstermektedir. PSD verilerinin sivri tepelerden ibaret olmasını sağlar. Bu sayede gelen verinin anlaşılması zorlaştırılır. Tablo 5.3'de PSD analizlerini ve tone jamming işlemi sonrası GPS sinyalinin değişimlerini görüntüleyebilirsiniz.

Tablo 5.3. Tone jamming sonrası GPS sinyali üzerinde gerçekleşen değişiklikler.

Jamming Katsayısı	GPS	PSD
0,0000		
0,0001		
0,0005		
0,0010		

Tone jamming işlemi sonrası GPS sinyallerinde oluşan sapma miktarları ve oluşturulan simülasyona dair konum grafikleri de Tablo 5.4'de gözükmektedir.

Tablo 5.4. Tone jamming sonrası rota üzerinde gerçekleşen değişiklikler.

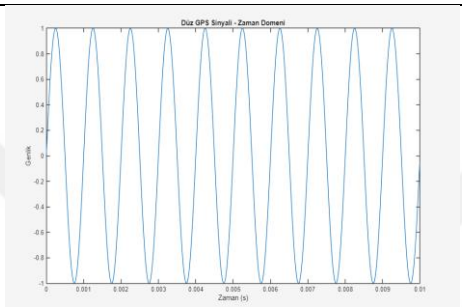
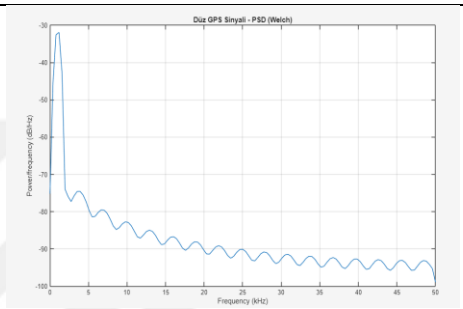
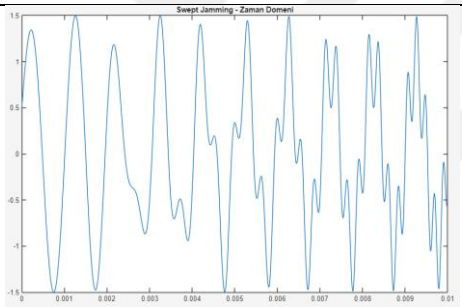
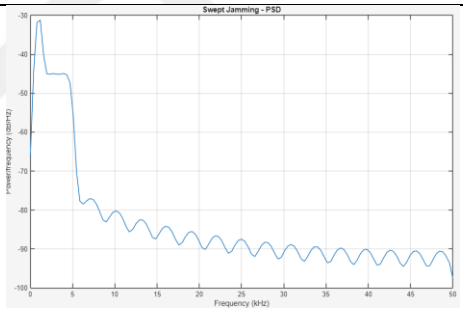
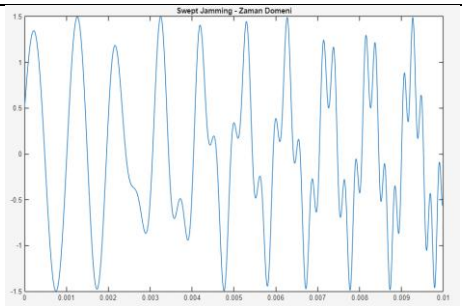
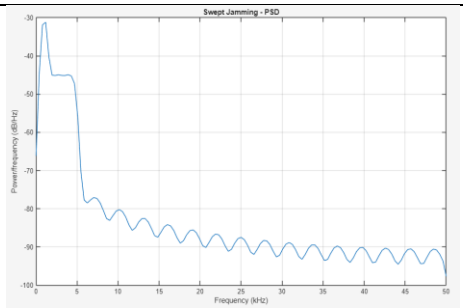
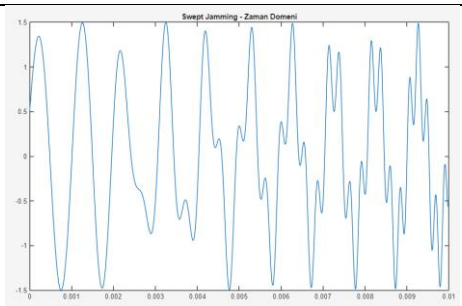
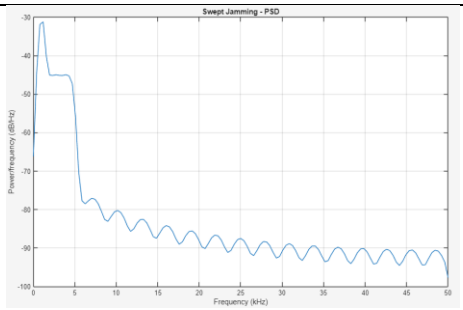
Jamming Katsayısı	**Sapma Miktarı (%)**	**Konum Grafiği**
0,0001	0.03	
0,0005	0.13	
0,0010	0.26	

Tone jamming işlemi sonrasında jamming katsayısı arttıkça tüm sinyaldeki sapma miktarı da artmaktadır. Jamming katsayısı 0,0010 olduğunda gerçek rotadan sapma miktarı % 26'ya kadar çıkmaktadır.

5.3. Swept Jamming İşleminin Farklı Katsayılar İle Birlikte GPS Sinyali Üzerindeki Etkisi

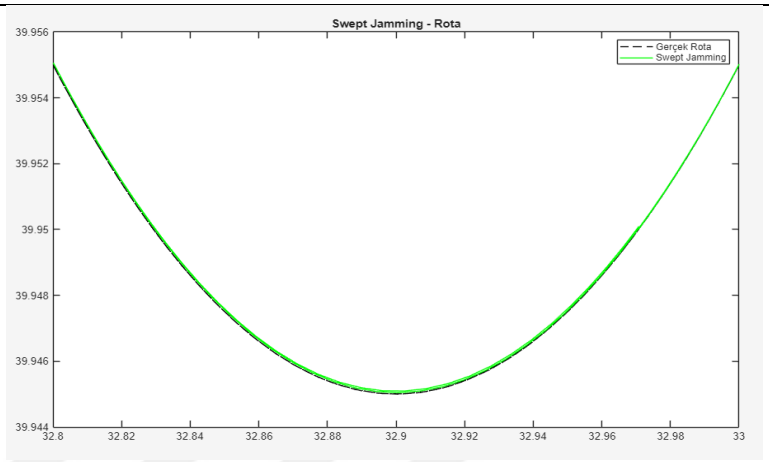
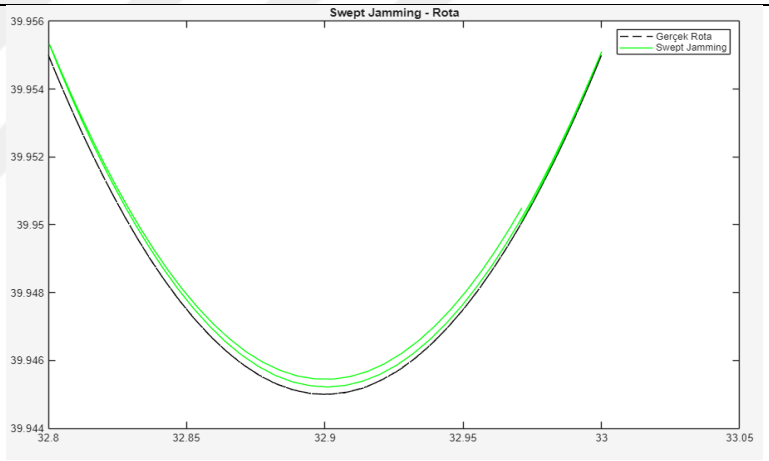
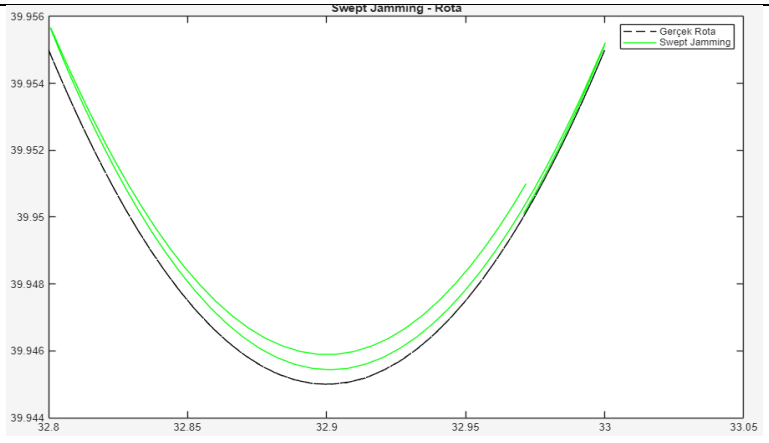
Swept jamming işlemi frekansı zamanla tarayarak sinyal bozma işlemi uygulamaktadır. Ayrıca saldırının sinyal tipi chirp biçimdedir. Dolayısıyla saldırı zamanla artan bir şekilde gerçekleşmektedir ve buda konuma lineer bir etkide bulunmaktadır. PSD verilerinin geniş ve düzgün olmasını sağlar. Bu sayede gelen verinin anlaşılması zorlaştırılır. Tablo 5.5'de PSD analizlerini ve swept jamming işlemi sonrası GPS sinyalinin değişimlerini görüntüleyebilirsiniz.

Tablo 5.5. Swept jamming sonrası GPS sinyali üzerinde gerçekleşen değişiklikler.

Jamming Katsayısı	GPS	PSD
0,0000		
0,0001		
0,0005		
0,0010		

Swept jamming işlemi sonrası GPS sinyallerinde oluşan sapma miktarları ve oluşturulan simülasyona dair konum grafikleri de Tablo 5.6'da gözükmektedir.

Tablo 5.6. Swept jamming sonrası rota üzerinde gerçekleşen değişiklikler.

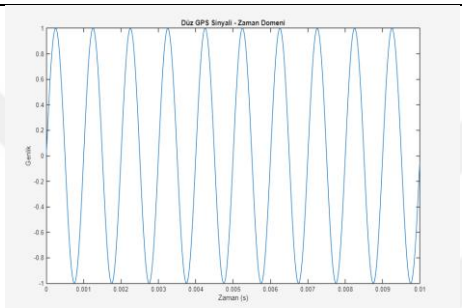
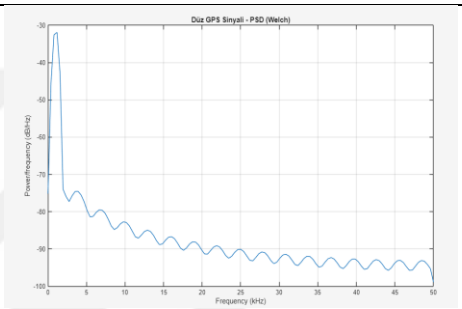
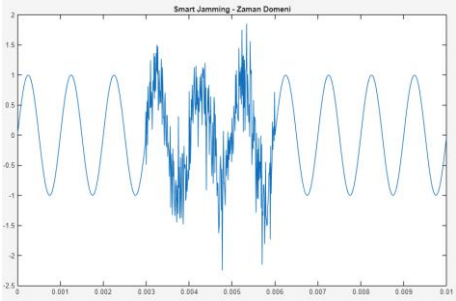
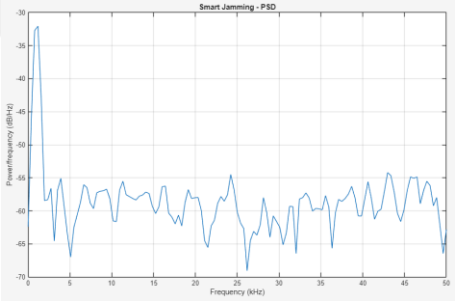
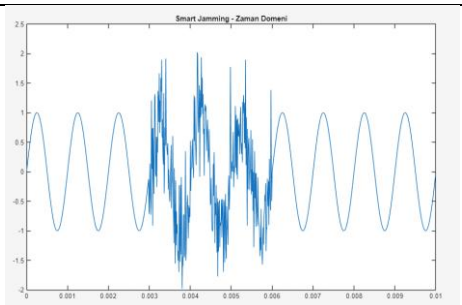
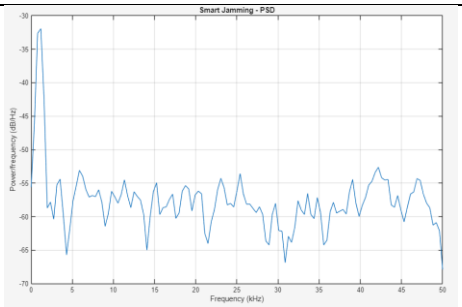
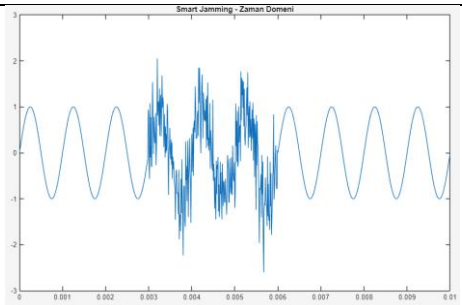
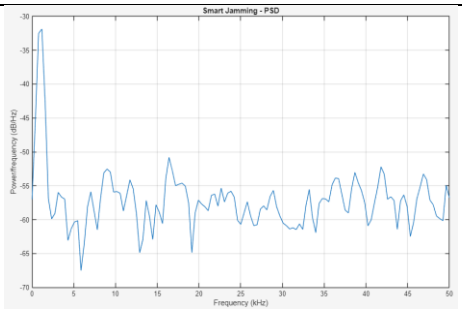
Jamming Katsayısı	**Sapma Miktarı (%)**	**Konum Grafiği**
0,0001	0.02	
0,0005	0.11	
0,0010	0.22	

Swept jamming işlemi sonrasında jamming katsayısı arttıkça tüm sinyaldeki sapma miktarı da artmaktadır. Jamming katsayısı 0,0010 olduğunda gerçek rotadan sapma miktarı % 22'ye kadar çıkmaktadır.

5.4. Smart Jamming İşleminin Farklı Katsayılar İle Birlikte GPS Sinyali Üzerindeki Etkisi

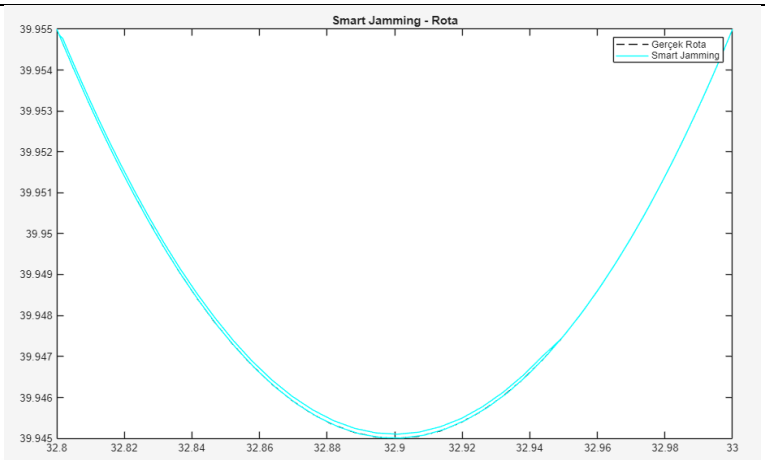
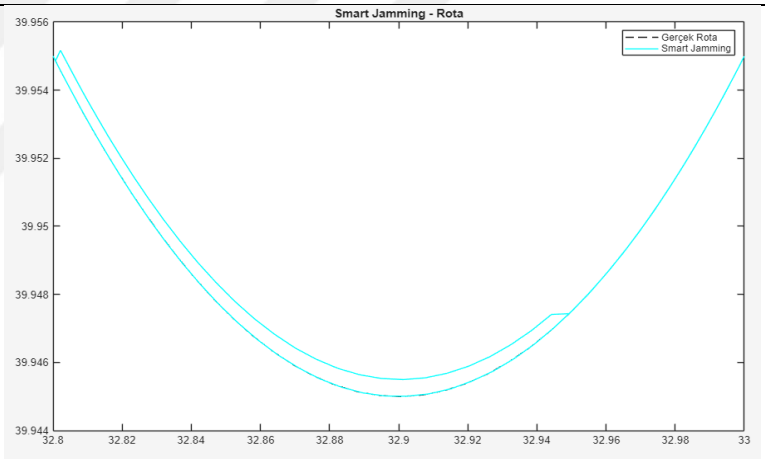
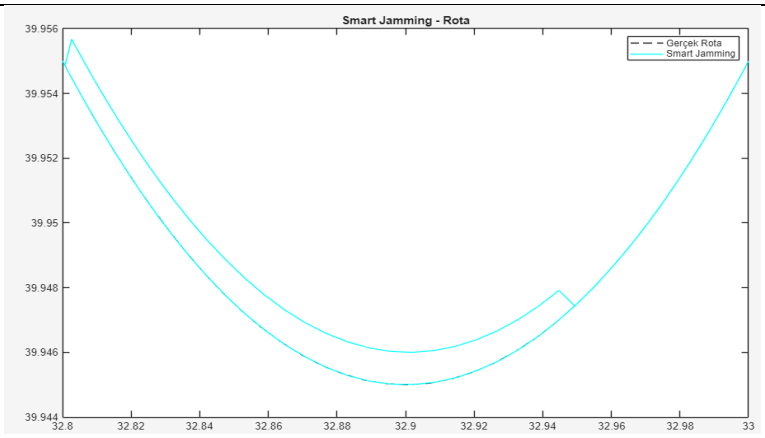
Smart jamming belirli bir bölgeye özel gürültü ekleyerek sinyal bozma işlemi uygulamaktadır. Dolayısıyla saldırı belirli bölgelerde gerçekleştiği için konum verisinde bölgesel sapmalar gerçekleşir. PSD verilerinin bölgesel artışlardan ibaret olmasını sağlar. Bu sayede gelen verinin anlaşılması zorlaştırılır. Tablo 5.7'de PSD analizlerini ve smart jamming işlemi sonrası GPS sinyalinin değişimlerini görüntüleyebilirsiniz.

Tablo 5.7. Smart jamming sonrası GPS sinyali üzerinde gerçekleşen değişiklikler

Jamming Katsayısı	GPS	PSD
0,0000		
0,0001		
0,0005		
0,0010		

Smart jamming işlemi sonrası GPS sinyallerinde oluşan sapma miktarları ve oluşturulan simülasyona dair konum grafikleride Tablo 5.8'de gözükmektedir.

Tablo 5.8. Smart jamming sonrası rota üzerinde gerçekleşen değişiklikler.

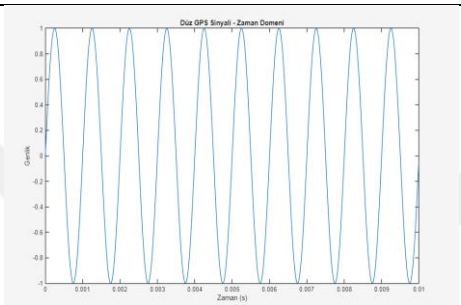
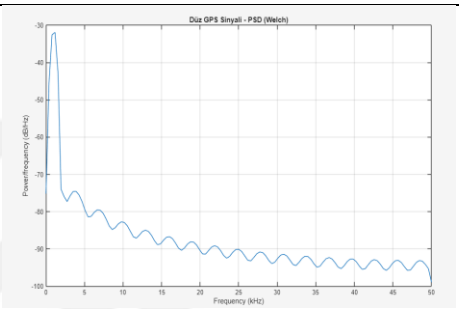
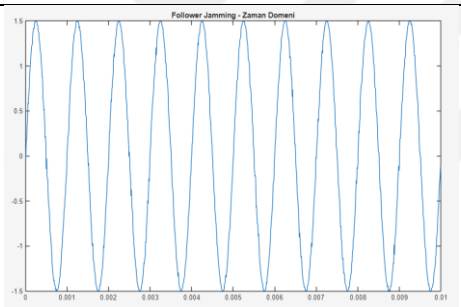
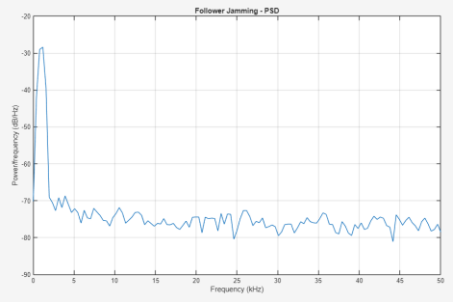
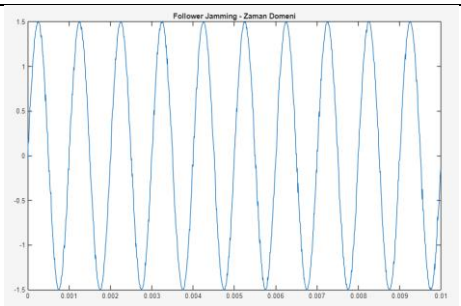
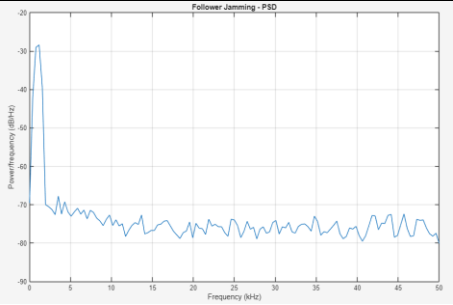
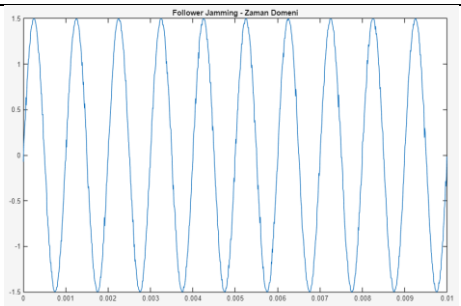
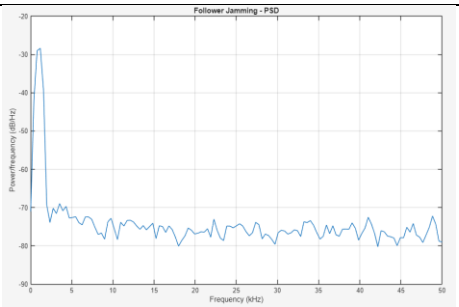
Jamming Katsayısı	**Sapma Miktarı (%)**	**Konum Grafiği**
0,0001	0.01	
0,0005	0.06	
0,0010	0.12	

Smart jamming işlemi sonrasında jamming katsayısı arttıkça tüm sinyaldeki sapma miktarı da artmaktadır. Jamming katsayısı 0,0010 olduğunda gerçek rotadan sapma miktarı % 12'ye kadar çıkmaktadır.

5.5. Follower Jamming İşleminin Farklı Katsayılar İle Birlikte GPS Sinyali Üzerindeki Etkisi

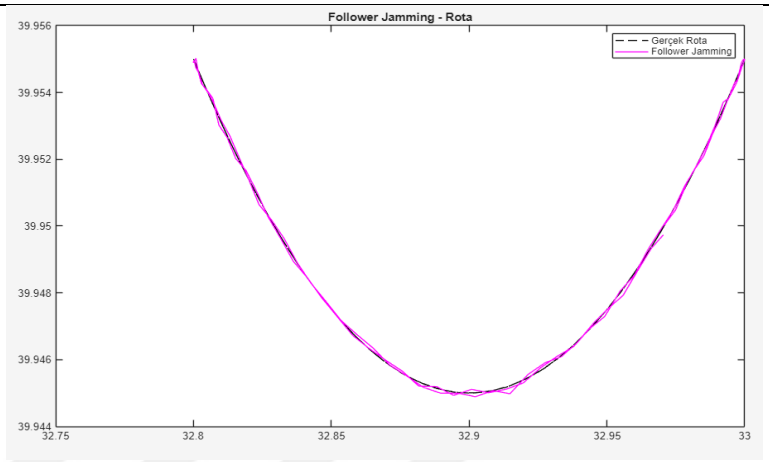
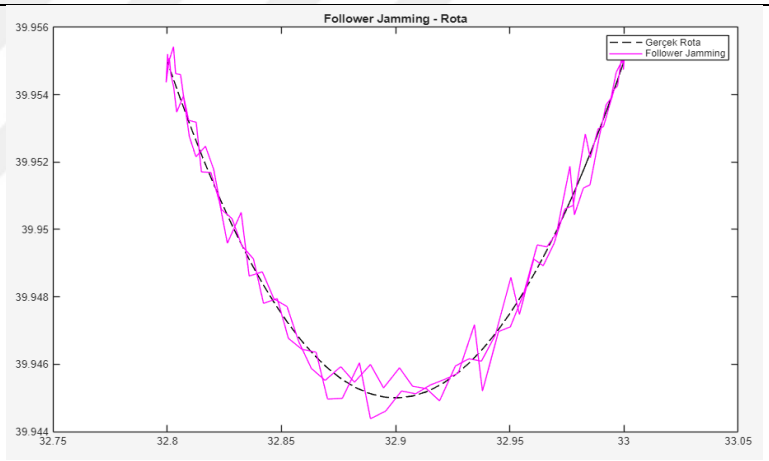
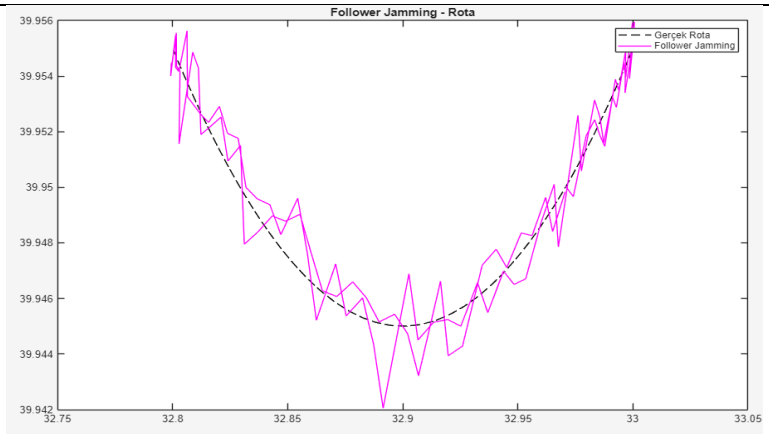
Follower jamming GPS sinyalini taklit ederek sinyal bozma işlemi uygulamaktadır. Dolayısıyla saldırı düşük sapma oranları ile gerçekleşir. PSD verilerinin GPS verilerine benzer olmasını sağlar. Bu sayede gelen verinin anlaşılması zorlaştırılır. Tablo 5.9'da PSD analizlerini ve follower jamming işlemi sonrası GPS sinyalinin değişimlerini görüntüleyebilirsiniz.

Tablo 5.9. Follower jamming sonrası GPS sinyali üzerinde gerçekleşen değişiklikler.

Jamming Katsayısı	GPS	PSD
0,0000		
0,0001		
0,0005		
0,0010		

Follower jamming işlemi sonrası GPS sinyallerinde oluşan sapma miktarları ve oluşturulan simülasyona dair konum grafikleri de Tablo 5.10'da gözükmektedir.

Tablo 5.10. Follower jamming sonrası rota üzerinde gerçekleşen değişiklikler.

Jamming Katsayısı	**Sapma Miktarı (%)**	**Konum Grafiği**
0,0001	0.03	
0,0005	0.15	
0,0010	0.33	

Follower jamming işlemi sonrasında jamming katsayısı arttıkça tüm sinyaldeki sapma miktarı da artmaktadır. Jamming katsayısı 0,0010 olduğunda gerçek rotadan sapma miktarı % 33'e kadar çıkmaktadır.

Günümüz savaş ortamında en güncel tehdit olarak görülen İHA'ların hassas noktalarından biri karıştırmadır. Bu karıştırma yöntemleri analiz edildiğinde her birinin farklı katsayılarda farklı etkileri olduğu gözlemlenmiştir. Ayrca karıştırmaya maruz kalınan süre ve karıştırmanın şiddeti GPS sistemlerinde ve İHA'ların rotalarında sapmalara sebep olacaktır. Burada incelemiş olduğumuz jamming türleri birbirleri ile kıyaslandığında, her birinin aynı jamming katsayılarında farklı sapma miktarları verdiği gözlemlenmiştir. Bu kapsamda; **Follower Jamming ve Noise Jamming** türlerinin GPS sinyalleri üzerindeki etkisi diğer jamming türlerine göre **daha fazla olduğu** gözlemlenmiştir. Teknolojik gelişmeler(anti-jam sistemleri vb.) ve kullanılan farklı navigasyon sistemleri bu jamming türlerinin İHA'lara etkisini azaltmayı veya hiç etkilemeden uçuşunu gerçekleştirmesini hedeflemektedir. Bu ve bunun gibi jamming türlerine maruz kalındığı fark edildiğinde o bölgeyi hızlı bir şekilde terk etmek en doğru hareket tarzı olacaktır.

6. SONUÇLAR

Bu çalışmada, İnsansız Hava Araçları (İHA) üzerindeki GPS engelleme ve karıştırma (jamming) tehditleri detaylı bir şekilde incelenmiştir. İHA'ların operasyonel etkinliği ve güvenilirliği için hayati önem taşıyan GPS sinyallerinin, dış müdahalelere karşı savunmasızlığı bu teknolojinin karşılaştığı en ciddi güvenlik zorluklarından biri olarak öne çıkmaktadır. Bu zafiyet, hem askeri hem de sivil uygulamalarda İHA'ların performansını olumsuz yönde etkileyebilmekte ve potansiyel olarak ciddi operasyonel riskler doğurabilmektedir.

GPS engelleme ve karıştırma teknikleri, İHA'ların temel görevlerini yerine getirmelerini engelleyerek, kontrol kaybı, yön sapması ve görev başarısızlığı gibi kritik sorunlara neden olmaktadır. Bu durum, sadece İHA'nın fiziksel güvenliğini tehlikeye atmakla kalmayıp, aynı zamanda görevlerin kritik zamanlarda aksamasına ve dolayısıyla daha geniş çaplı olumsuz sonuçlara yol açabilmektedir. Örneğin, askeri keşif ve gözetim faaliyetlerinde GPS sinyallerinin karıştırılması, düşman unsurların İHA'nın rotasını değiştirmesine ya da tamamen devre dışı kalmasına imkân tanırken, sivil uygulamalarda acil durum müdahale ekiplerinin hızlı ve doğru karar vermesini engelleyebilir. Tarım, lojistik ve afet yönetimi gibi alanlarda da GPS sinyal bozulmaları, ekonomik kayıplara ve insan hayatını doğrudan etkileyen aksaklıklara neden olabilmektedir.

Bu çalışmada ele alınan literatür taraması ve teknik analizler, GPS engelleme tehdidinin hem teknoloji hem de güvenlik perspektiflerinden çok boyutlu bir sorun olduğunu göstermiştir. Mevcut savunma teknikleri ve karşı tedbirler, bu tehdidin etkilerini azaltmaya yönelik önemli adımlar olsa da, gelişen elektronik harp teknolojileri karşısında sürekli bir yenilenme ve geliştirme gerektirmektedir. Özellikle, sinyal işleme algoritmalarının iyileştirilmesi, yapay zekâ destekli anomali tespit sistemlerinin kullanımı, entegre navigasyon çözümlerinin geliştirilmesi ve alternatif konumlama sistemlerinin entegre edilmesi, İHA'ların GPS karıştırma saldırılarına karşı dayanıklılığını artırmak için kritik stratejiler olarak ön plana çıkmaktadır.

Ayrıca, bu alanda yapılan yeni araştırmalar, GPS karıştırma ve spoofing saldırılarının sadece teknik bir sorun olmanın ötesinde, ulusal güvenlik, stratejik savunma politikaları ve siber güvenlik alanlarında da önemli etkiler doğurduğunu ortaya koymaktadır. Dolayısıyla, İHA güvenliğinin sağlanması sadece mühendislik problemlerinin çözümüyle değil, aynı zamanda kapsamlı politikalar ve standartların oluşturulmasıyla da desteklenmelidir.

Sonuç olarak, İHA teknolojilerinin giderek yaygınlaştığı ve kritik görevlerde vazgeçilmez hale geldiği günümüzde, GPS engelleme ve karıştırma tehditlerine karşı etkin önlemlerin geliştirilmesi ve uygulanması kaçınılmazdır. Bu çalışma, İHA operatörlerine, güvenlik uzmanlarına ve araştırmacılara, bu karmaşık tehdidi anlamaları ve etkili çözümler geliştirmeleri için sağlam bir temel sunmayı amaçlamaktadır. Gelecekte yapılacak çalışmaların, bu alandaki teknolojik gelişmelerle paralel olarak, İHA'ların güvenilirliğini artıracak yenilikçi savunma mekanizmalarını ortaya koyması beklenmektedir.

Bu bağlamda, GPS karıştırma ve engelleme gibi elektronik saldırılara karşı sürekli gelişen tehdit ortamına uyum sağlayabilen, çok katmanlı ve esnek güvenlik stratejilerinin geliştirilmesi, İHA teknolojilerinin sürdürülebilir ve güvenli bir şekilde kullanılabilmesinin temel koşulu olacaktır.

KAYNAKLAR

[1] M. Psiaki and T. Humphreys, "Civilian GNSS Spoofing, Detection, and Recovery," *Integrated Satellite Navigation, Sensor Systems, and Civil Applications,* no. Position, Navigation, and Timing Technologies in the 21st Century, 2021.

[2] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," *International Journal of Navigation and Observation,* 2012.

[3] C. Günther, "A Survey of Spoofing and Counter-Measures," *Journal of the Institute of Navigation,* vol. 61, no. 3, pp. 159-177, 2014.

[4] S. Z. Khan, M. Mohsin and W. Iqbal, "On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions," *PeerJ Computer Science,* no. doi: 10.7717/peerj-cs.507, 6 May 2021.

[5] Austin, R. (2010). Unmanned Aircraft Systems: UAVs Design, Development and Deployment. John Wiley & Sons.

[6] Clough, B. T. (2002). Metrics, Schmetrics! How the Heck Do You Determine a UAV's Autonomy Anyway Proceedings of the Performance Metrics for Intelligent Systems Workshop.

[7] Floreano, D., & Wood, R. J. (2015). Science, technology and the future of small autonomous drones. Nature, 521(7553), 460–466.

[8] DGCA RPAS Guidance Manual, [Online]. Available:https://public-prd-dgca.s3. ap-south1.amazonaws.com/InventoryList/headerblock/drones/DGCA%20RPAS%20Guidance%20Manual.pdf.

[9] B. Hofmann-Wellenhof, Herbert Lichtenegger, and J. Collins. Global Positioning System 2001.

[10] A. El-Rabbany. Introduction to GPS: The Global Positioning System. Artech House mobile communications series. Artech House, Boston, Mass. and London, 2002. ISBN 1-58053-183-0.

[11] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle. GNSS–Global Navigation Satellite Systems: GPS, Glonass, Galileo, and more. Springer,Wien and New York, 2008.

[12] J. J. Spılker. GPS Signal Structure and Performance Characteristics. Navigation, 25(2):121–146, 1978.

[13] Sadeghi M. and Gholami M. Time Synchronizing Signal By GPS Satellites. 2008.

[14] Sadeghi M. and Gholami M. Time Synchronizing Signal by GPS Satellites. Dept. Of Electrical Engineering University of Azad Eslamshahr branch, 2008.

[15] E.D. Kaplan, C. Hegarty, Understanding GPS/GNSS: Principles and applications. Artech house, 2017.

[16] J. Sanz, J. M. Juan, and M. Hernández-Pajares. "GNSS Data Processing, Volume I: *Fundamentals and Algorithms*." (2013).

[17] GPS: The Global Positioning System, https://www.gps.gov/ (Erişim tarihi: 18 Nisan 2023).

[18] Chamola V., Kotesh P., Agarwal A., Gupta N., Guizani M., "A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques" Ad Hoc Networks 111 (2021) 1-20.

[19] L. Liu, G. Han, S. Chan, M. Guizani, An snr-assured anti-jamming routing protocol for reliable communication in industrial wireless sensor networks, IEEE Communications Magazine 56 (2) (2018) 23–29.

[20] R.A. Poisel, Modern Communications Jamming Principles and Techniques, 2nd, Artech House, Inc., USA, 2011.

[21] Y. Junfei, L. Jingwen, S. Bing, J. Yuming, Barrage jamming detection and classification based on convolutional neural network for synthetic aperture radar. IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium, 2018, pp. 4583–4586, https://doi.org/10.1109/IGARSS.2018.8519373.

[22] L. Ma, C. Fan, W. Sun, G. Qiao, Comparison of jamming methods for underwater acoustic dsss communication systems. 2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC), 2018, pp. 1340–1344, https://doi.org/10.1109/IMCEC.2018.8469430.

[23] D. Borio, Swept gnss jamming mitigation through pulse blanking. 2016 European Navigation Conference (ENC), 2016, pp. 1–8, https://doi.org/10.1109/ EURONAV.2016.7530549.

[24] M.T. Gamba, E. Falletti, Performance analysis of fll schemes to track swept jammers in an adaptive notch filter. 2018 9th ESA Workshop on Satellite NavigationTechnologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 2018, pp. 1–8, https://doi.org/10.1109/ NAVITEC.2018.8642663.

[25] C.C. Ko, H. Nguyen-Le, L. Huang, Ml-based follower jamming rejection in slow fh/ mfsk systems with an antenna array, IEEE Transactions on Communications 56 (9) (2008) 1536–1544.

[26] K. Parlin, M. Alam, Y. Le Moullec, Jamming of uav remote control systems using software defined radio. Jamming of UAV Remote Control Systems Using Software Defined Radio, 2018, https://doi.org/10.1109/ICMCIS.2018.8398711.

[27] A. Pinker, C. Smith, Vulnerability of the gps signal to jamming, GPS Solutions 3 (2) (1999) 19–27

ÖZGEÇMİŞ

Mehmet ÇIRAK

[redacted]

[redacted]

ARAŞTIRMACI BİLGİLERİ

Öğrenci Orcid ID : 0000-0003-0330-7801
Danışman Orcid ID : 0000-0001-9623-2284

[redacted]

ARAŞTIRMA DENEYİMİ

İŞ DENEYİMİ

AKADEMİK FAALİYETLER

Bildiriler:

1. M. Cirak, O. Yaman, "Research of GPS Jammıng Methods in Unmanned Aerıal Vehıcles", 7th Internatıonal Anatolıan Scıentıfic Research Congress, Munzur University, Tunceli, 17-18 April, 2025.