
GAZİ ÜNİVERSİTESİ
Gazi
1926

İNSANSIZ HAVA ARAÇLARINDA GPS ALDATMACASI TESPİTİ

Emre UYAR

YÜKSEK LİSANS TEZİ
BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

EKİM 2019

Emre UYAR tarafından hazırlanan "İNSANSIZ HAVA ARAÇLARINDA GPS ALDATMACASI TESPİTİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. İbrahim Alper DOĞRU

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ..……

Başkan: Prof. Dr. Türksel KAYA BENSGHİR

İktisadi ve İdari Bilimler Fakültesi/İşletme Bölümü, Ankara Hacı Bayram Veli Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ...……

Üye: Prof. Dr. Ercan Nurcan YILMAZ

Elektrik-Elektronik Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ...……

Tez Savunma Tarihi: 09/10/2019

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..…….

Prof. Dr. Sena YAŞYERLİ

Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Emre UYAR

09/10/2019

İNSANSIZ HAVA ARAÇLARINDA GPS ALDATMACASI TESPİTİ

(Yüksek Lisans Tezi)

Emre UYAR

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Ekim 2019

ÖZET

İnsansız Hava Araçları (İHA) günümüzde yaygın olarak kullanılmaktadır. Bu araçlar askeri alanda kullanılmasının yanında afet kurtarma, hassas tarım ve hobi gibi çeşitli amaçlar için de tercih edilmektedir. Küresel Konumlandırma Sistemi (Global Positioning System - GPS), hassas konum ve otonom uçuş yeteneği sunmasından dolayı bu araçlar için önemli bir bileşendir. Teknolojinin hızla gelişmesiyle birlikte bu sistemlerin sivil alanda da kullanımı oldukça artmıştır. Ancak sivil GPS sinyali, yapısının açık ve şifresiz olması sebebiyle aldatmaca saldırılarına karşı savunmasızdır. Bu çalışmada, GPS aldatmacasının tespiti ve önlenmesine yönelik literatürdeki çalışmalar incelenmiştir. GPS aldatmacası saldırıları sonucunda, İHA'lar ele geçirilerek veya düşürülerek maddi kayıplara sebebiyet verilebilmektedir. Yakın gelecekte GPS aldatmacası saldırı çeşitliliğinin ve tespit yöntemlerinin artacağı öngörülmektedir. İHA üzerinde bulunun Ataletsel Ölçüm Birimi – AÖB (Inertial Measurement Unit - IMU) sensör verileri ve diğer Küresel Uydu Seyrüsefer Sistemleri (Global Navigation Satellite System - GNSS) verileri karşılaştırılarak optimum tespit sistemi tasarlanmıştır. Araştırmacılar için GPS aldatmacası tespitine yönelik verimli bir kaynak sunulmuştur. İlerleyen zamanda söz konusu sisteme ek olarak, GPS aldatmacası saldırısı sonucunda hava araçlarının tam kontrolünün sağlanmasına yönelik çalışmalara devam edilecektir.

Bilim Kodu	:	92429
Anahtar Kelimeler	:	GPS Aldatmacası, İnsansız Hava Aracı, Aldatmaca Tespiti, GNSS, Siber Güvenlik
Sayfa Adedi	:	59
Danışman	:	Doç. Dr. İbrahim Alper DOĞRU

DETECTION OF GPS SPOOFING ON UNMANNED AERIAL VEHICLES

(M. Sc. Thesis)

Emre UYAR

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

October 2019

ABSTRACT

Unmanned Aerial Vehicles (UAV) are widely used today. These vehicles are used in military fields as well as for various purposes such as disaster recovery, sensitive agriculture, and hobby. Global Positioning System (GPS) is an indispensable component for UAVs. These technologies have enormous priority because they produce precise position knowledge and autonomous flight capability. In recent years, as a result of the rapid development of technology, the use of GPS in the civilian field has remarkably increased. However, the civilian GPS signal is vulnerable to spoofing attacks because its structure is clear and unencrypted. In this work, the studies in the literature regarding the detection and prevention of GPS spoofing have been researched. As a result of GPS spoofing attacks, the UAVs can be seized or dropped to cause material losses. It is predicted that GPS spoofing attack variety and detection methods will increase in the near future. The optimum detection system has been designed by comparing the Inertial Measurement Unit (IMU) sensor data and other Global Navigation Satellite System (GNSS) data on the UAV. This study provides an efficient source of GPS spoofing detection for researchers. In addition to this system, studies are planned to continue on ensuring full control of aerial vehicles after a successful GPS spoofing attack is ensured.

Science Code : 92429
Key Words : GPS Spoofing, Unmanned Aerial Vehicle, Spoofing Detection, GNSS, Cyber Security
Page Number : 59
Supervisor : Assoc. Prof. Dr. İbrahim Alper DOĞRU

TEŞEKKÜR

Çalışmalarım süresince tez danışmanlığımı üstlenerek bana yol gösteren, çalışmanın yürütülmesinde katkı ve destek sunan değerli sayın hocalarım; Doç. Dr. İbrahim Alper DOĞRU ve Öğr. Gör. Dr. Murat DÖRTERLER'e teşekkür ederim. Desteklerinden dolayı çok değerli aileme ayrıca teşekkür ederim.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklamalar**
Ghz	Gigahertz
Mhz	Megahertz

Kısaltmalar	**Açıklamalar**
ABD	Amerika Birleşik Devletleri
AGC	Automatic Gain Control
AÖB	Ataletsel Ölçüm Birimi
APM	ArduPilot Mega
CNAV	Civil Navigation
DDoS	Distributed Denial of Service
DoS	Denial of Service
EUROUVS	European Association of Unmanned Vehicle Systems
GALILEO	European Global Satellite Navigation System
GLONASS	Globalnaya Navigazionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HALE	High-Altitude Long Endurance
ICMP	Internet Control Message Protocol
İHA	İnsansız Hava Aracı
IMU	Inertial Measurement Unit
IRNSS	Indian Regional Navigation Satellite System
LEN	Lenght
LK	Lucas-Kanade
LTE	Long-Term Evolution
MALE	Medium-Altitude Long Endurance
MAVLink	Micro Air Vehicle Link

Kısaltmalar	Açıklamalar
PRN	Pseudo Random Number
PVT	Position Velocity Time
RAIM	Receiver Autonomous Integrity Monitoring
RC	Remote Control
RF	Radio Frequency
RMSE	Root Mean Square Error
SDR	Software-Defined Radio
SEQ	Sequence
SNR	Signal-to-Noise Ratio
SVM	Support Vector Machine
SYN	Synchronize
TOA	Time of Arrival
TSARM	Time Synchronization Attack Rejection and Mitigation
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
Wi-Fi	Wireless Fidelity

1. GİRİŞ

İHA'lar askeri amaçlarla kullanıldığı gibi felaket kurtarma, hassas tarım, trafik izleme ve hobi amaçlı olarak hayatımızın birçok alanında karşımıza çıkmaktadır. Söz konusu hava araçları tarafından kontrol ve veri iletimi amaçlarıyla Radyo Frekansı, Wi-Fi, Bluetooth, 3G/4G/LTE ve GPS gibi çeşitli kablosuz haberleşme teknolojileri kullanılmaktadır [1]. Küresel konumlandırma sistemleri İHA'lar için hassas konum bilgisi sağlamasından dolayı büyük bir öneme sahiptir.

GPS, ilk olarak yalnızca askeri kullanımlara açık iken 1980 yılından itibaren sivil kullanıma da açılmıştır [2]. Günümüzde ise konum, hız ve zaman gibi bilgilere ihtiyaç duyulan gerek endüstriyel gerekse de eğlence amaçlı birçok uygulamada kullanılır duruma gelmiştir. GPS sinyalleri, jamming (engelleme/kesme), spoofing (aldatmaca) saldırıları ve radyo frekansı (Radio Frequency - RF) paraziti gibi çevresel faktörler tarafından etkilenmektedir. GPS aldatmacası belirtilen etkenlerden dolayı en tehlikeli ve tespit edilmesi en zor olan saldırı yöntemi olarak dikkat çekmektedir.

GPS aldatmacası saldırısının en bilinen örneği olarak, 2011 yılında Amerikan Hava Kuvvetleri'ne ait RQ-170 Sentinel insansız hava aracının Afganistan sınırında düşürülmesi gösterilmektedir [3]. Düşürülen hava aracına ait görüntülerin yayımlanmasının ardından İranlı mühendislerin GPS sisteminin zayıflığından bahsetmeleri üzerine akademik alanda GPS sistemine yönelik birçok araştırma yapılmıştır. Yapılan araştırmalar sonucunda GPS aldatmacasının hedef hava aracı üzerinde etkili olduğu kanıtlanmıştır.

GPS sistemi yönetiminin Amerika Birleşik Devletlerinde (ABD) olması ve özellikle sivil alanda yapısı gereği saldırılara karşı korumasız olması sebebiyle farklı ülkeler tarafından çeşitli küresel konumlandırma sistemi projeleri geliştirilmektedir. Rusya tarafından geliştirilen GLONASS (Global Navigation Satellite System), Avrupa Birliği tarafından geliştirilen Galileo, Çin tarafından geliştirilen BeiDou ve Hindistan tarafından geliştirilen IRNSS (The Indian Regional Navigation Satellite System) konumlandırma sistemleri mevcuttur. Ancak GPS dışındaki sistemler, henüz yeterli olgunluk seviyesine ulaşamadığı için dünya genelinde ağırlıklı olarak neredeyse her alanda GPS kullanılmaktadır [4].

Bu tezde, yaygın kullanımından dolayı İHA'lardaki GPS sistemlerinin güvenlik zafiyetleri araştırılmıştır. Özellikle yapısının açık, şifresiz olması ve herhangi bir kimlik doğrulama mekanizmasına sahip olmamasından dolayı sivil GPS sinyallerine odaklanılmıştır. GPS aldatmacası tespiti ve önlenmesine yönelik literatürdeki çeşitli çalışmalar incelenmiştir. Son zamanlarda hızlı gelişen teknolojiyle birlikte söz konusu sistemlere yönelik saldırı çeşitliliğinin ve bu saldırıların tespit yöntemlerinin artacağı öngörülmektedir.

GPS aldatmacası tespiti için literatürdeki çalışmalarda genellikle sinyal işleme, veri biti, pozisyon ve navigasyon çözümü katmanlarında çalışmalar gerçekleştirilmiştir. İHA'nın üzerindeki mevcut donanımları kullanması ve herhangi bir harici donanıma ihtiyaç duymandan yer kontrol istasyonu üzerinden hızlı bir şekilde analiz imkânı sunmasından dolayı pozisyon ve navigasyon seviyesindeki çalışmalara odaklanılmıştır. AÖB sensörlerinden alanın veri ve diğer GNSS sistemlerinden alınan verilerinin karşılaştırmalı analizinden hibrit bir GPS aldatmacası tespit sistemi üzerinde çalışmalar gerçekleştirilmiştir. İkinci bölümde literatürde yer alan çalışmalar analiz edilmektedir. Üçüncü bölümde insansız hava araçları; sınıfları, haberleşme yöntemleri ve müdahale yöntemleri açısından incelenmektedir. Dördüncü bölümde İHA sistemlerine yönelik başlıca siber tehditler ve alınması gereken önlemler belirtilmektedir. Beşinci bölümde GPS ve diğer küresel konumlandırma sistemleri ile GPS'in bilinen açıklıkları ve GPS aldatmacası tespit yöntemlerinden bahsedilmektedir. Altıncı bölümde GPS aldatmacası tespiti için gerçekleştirilen analiz çalışmaları sunulmaktadır. Son bölümde ise elde edilen sonuçlar değerlendirilerek, sonraki araştırmacılar için çalışma alanları önerilmektedir.

2. LİTERATÜRDE YER ALAN ÖNCEKİ ÇALIŞMALAR

İHA'lara yönelik gerçekleştirilen GPS aldatmacası saldırılarının tespit edilmesi ve tespit edilen saldırıların engellenmesi başta olmak üzere çeşitli konularda makaleler incelenmiştir.

Qiao ve arkadaşları tarafından 2017 yılında yapılan çalışmada, GPS aldatmacasını tespit etmek amacıyla dronun monocular (yüksek zoom özellikli) kamera ve AÖB/IMU (Inertial Measurement Unit: Accelerometers, Gyroscopes, Magnetometers) sensörlerinden alınan veriler kullanılmıştır. Söz konusu sensörlerden hava aracının hız ve pozisyon bilgisi alınmıştır. Ayrıca GPS ve bir önceki pikselden bir sonraki pikseli tahmin etme yöntemine dayalı hız tespiti için kullanılan LK (Lucas-Kanade) metotlarıyla ortalama 5 saniye içerisinde aldatmaca tespiti gerçekleştirilmiştir. Önerilen yöntemin, yalnızca AÖB'nin kullanımından daha etkili olduğu belirtilmektedir [5].

Su ve arkadaşları tarafından 2016 yılında yapılan çalışmada, hata detektörü ile donatılmış bir insansız hava aracını, GPS aldatmacası ile yönlendirmeye yönelik bir senaryo belirtilmiştir. GPS ölçümündeki anlık değişimleri hesaplamak için etkili bir çözüm sağlandığı iletilmektedir. GPS aldatmacası saldırısı yoluyla birleşik skaler test hata detektörü ile donatılmış hava aracının gerçek zamanlı olarak manipüle edilmesi yöntemi araştırılmıştır [6].

Huang ve arkadaşları tarafından 2016 yılında yapılan çalışmada, kurban alıcısının gerçek ve yanlış sinyaller arasında ayrım yapamadığı ve kullanıcıyı bu konuda uyaramadığı vurgulanmaktadır. Söz konusu çalışmada, sinyal ilişkilendirilmesinde olası bozulmaları izlemeye izin veren "Ratio Test" yöntemi ile aldatmaca tespitinin etkinliği ve verimliliği araştırılmıştır. Ratio Test ile sinyal bozulmalarından GPS aldatmaca saldırılarının başarılı bir şekilde tespit edildiği belirtilmektedir [7].

Wesson ve arkadaşları tarafından 2017 yılında yapılan çalışmada, GPS ve diğer küresel konumlandırma uydu sistemi alıcılarıyla, aldatmaca ve engelleme/kesme saldırılarının algılanmasını sağlayan düşük maliyetli bir teknik önerildiği belirtilmektedir. Güç Bozulma Detektörü (Power Distortion Detector) olarak adlandırılan bu teknik, alınan güç ve

korelasyon fonksiyonu bozulmalarına göre sinyalleri; Çok Yollu Sarsılmış (Multipath-afflicated), Aldatılmış (Spoofed) ve Engellenmiş/Kesilmiş (Jammed) olarak sınıflandırmaktadır. Saldırı ve saldırı dışı senaryoların 27 yüksek kaliteli deneysel kayıtları üzerinde gerçekleştirilen farklı testlerde; detektör tarafından %0,5 hata oranıyla aldatmaca ve engelleme saldırılarının tespit edildiği belirtilmektedir. Ayrıca uygulamaya ait yazılım kodlarının "Github" üzerinden sunulduğu bilgisi iletilmektedir [8].

He ve arkadaşları tarafından 2014 yılında yapılan çalışmada, başarılı aldatmaca saldırıları için teorik bir model sunulmaktadır. Sinyal gücünün, alıcının izleme halkalarına etkisi analiz edilerek çeşitli nicel analizler gerçekleştirilmektedir. Aldatmaca sinyalinin gücü, gerçek sinyalin gücüne eşit olduğunda sinyaller arasında faz hizalanması gerçekleştiği, sonrasında sahte sinyalin gücünü artırarak gerçek sinyalden uzaklaştığı ve izleme döngüsünü ele geçirdiği belirtilmektedir [9].

Kerns ve arkadaşları tarafından 2014 yılında yapılan çalışmada, GPS sinyal aldatmacası ile insansız hava aracı yakalama ve kontrol teorisine yönelik uygulama analiz edilmiştir. Genişletilmiş Kalman Filtresi (Extended Kalman Filter), GPS verilerini tahmin etmek amacıyla kullanılmıştır. Hava aracı ve aldatıcının birbirine bağlı dinamikleri analiz edilerek, GPS aldatmacası saldırısı ile bir hava aracının kabul edilen bir yörüngesinin bilinmeden takip edebileceği belirtilmiştir. Sonuç olarak, arazi testleriyle insansız hava araçlarına karşı GPS aldatmacası saldırısının hem teknik hem de operasyonel olarak mümkün olduğu vurgulanmaktadır [10].

Khalajmehrabadi ve arkadaşları tarafından 2017 yılında yapılan çalışmada, GPS üzerinden zaman senkronizasyonu saldırıları için TSARM (Time Synchronization Attack Rejection and Mitigation) tekniği tanıtılmaktadır. Söz konusu teknikte, anlık zaman tahmini yapılarak saat ve alıcı sapmasının düzeltildiği belirtilmektedir. Ayrıca sayısal sonuçların literatürdeki rakip yaklaşımlara göre TSARM tekniğinin önde olduğunu gösterdiği vurgulanmaktadır [11].

Panice ve arkadaşları tarafından 2017 yılında yapılan çalışmada, anomali tespiti için veri sınıflandırma amacıyla makine öğrenmesinde kullanılan SVM (Support Vector Machine) yöntemiyle durum tahmini analizine dayanarak, GPS aldatmacası tespiti için yeni bir yaklaşım getirildiği vurgulanmaktadır. Söz konusu yöntemde hava aracı üzerinde ilave bir

donanıma ihtiyaç duyulmadığı belirtilerek, analizin AÖB sensörleriyle birlikte kullanılması durumunda performansın artacağı iletilmektedir. Çalışma neticesinde, Matlab kullanılarak GPS verileri işlenmiş ve 30 saniye içerisinde GPS aldatmacası tespiti gerçekleştirilmiştir [12].

O'Hanlon ve arkadaşları tarafından 2013 yılında yapılan çalışmada, iki dar bantlı sivil alıcılardan, şifrelenmiş GPS L1 P(Y) kod sinyalleri arasındaki korelasyonlar kullanarak, GPS aldatmacasının tespiti yapılmaktadır. Söz konusu alıcılardan birinin aldatmacaya maruz kalmayan, güvenli bir yerde olduğu varsayılırken diğer alıcının ise aldatmaca saldırısına maruz bırakıldığı varsayılmaktadır. C/A ve P(Y) kod sinyalleri arasındaki güç farklılıkları deneysel olarak araştırılmıştır. Araştırma sonucuna göre başarılı bir şekilde aldatmaca tespiti yapıldığı belirtilmektedir [13].

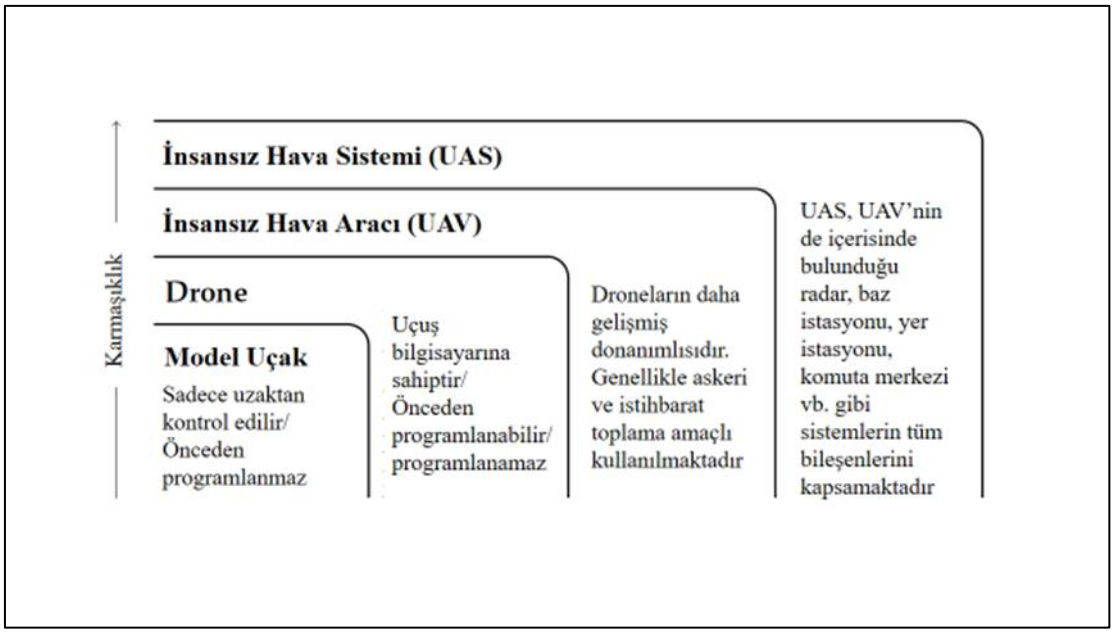
Psiaki ve Humphreys tarafından 2016 yılında yapılan çalışmada, kurban bir GPS alıcısını; pozisyon ve saat ofseti hakkında aldatmak için kullanılabilecek bir dizi saldırı stratejisi anlatılmaktadır. Söz konusu stratejilerin bir kısmında sinyallerdeki anomalileri bulmak için sinyal işleme kullanılmaktadır. Özellikle bir saldırı tespit edildikten sonra navigasyonun nasıl kurtarılacağı sorusuyla, aldatmacaya karşı savunma alanında daha fazla araştırma ve geliştirmeye ihtiyaç duyulduğu belirtilmektedir [14].

3. İNSANSIZ HAVA ARAÇLARI

Günümüzde İHA'lar giderek yaygınlaşmaktadır. Bu araçlar, askeri amaçlarla kullanıldığı gibi oyun, hobi, iş, felaket kurtarma, hassas tarım gibi birçok alanda kullanılabilmektedir. Hatta online alışveriş sitesi Amazon, prime hizmeti olarak yaklaşık 13 dolar karşılığında satılan ürünleri İHA'lar ile alıcılarına ulaştırmaktadır [15]. Sınırdan ilaç kaçırma, pokemon go oyunu oynama ve Beyaz Saray etrafında dolaşarak görüntü alma gibi çeşitli kullanım örnekleri, çeşitli zamanlarda ulusal ve uluslararası basının gündemine oturmuştur. Yine İran tarafından ele geçirilen Amerikan insansız hava araçları durumun ciddiyetini ve bu araçların önemini gözler önüne sermektedir [16, 17].

3.1. İnsansız Hava Araçları Sınıfları

İHA'lar çeşitli özelliklere göre sınıflandırılmaktadır. Eğlence amaçlı olarak model uçaklar kullanılırken, biraz daha gelişmiş, uçuş bilgisayarı içeren ve önceden programlanabilen dronlar; izleme, takip, afet kurtarma, vb. amaçlarla kullanılabilmektedir. Genellikle askeri amaçlarla kullanılan ve dronların daha gelişmişi İHA'lar, askeri istihbarat faaliyetleri için tercih edilmektedir. Günümüzde artık İHA sistemleri silahlarla donatılmıştır. Bu sayede istihbaratın yanında saldırı da yapabilmektedir. İHA'ların da içinde yer aldığı radar, baz istasyonu, yer istasyonu, komuta merkezi, vb. gibi sistemlerin bir araya gelmesiyle insansız hava sistemleri (Unmanned Aerial Systems - UAS) oluşmaktadır. Şekil 3.1'de insansız hava araçlarının kullanım amaçlarına göre sınıflandırılması sunulmaktadır [16, 17].



Şekil 3.1. İnsansız hava araçlarının sınıflandırılması [17, 18]

Askeri amaçlarla Avrupa'da İHA üreticileri tarafından oluşturulan lobinin (EUROUVS) yaptığı sınıflandırma Çizelge 3.1'de sunulmaktadır. Micro, Mini ve Close Range İHA'lar genellikle teknoloji marketlerde satılan; Dji, Phantom ve benzeri markalar tarafından üretilen, video çekimleri gibi sosyal amaçlarla kullanılan hava araçlarıdır. Orta İrtifa Uzun Havada Kalış (Medium-Altitude Long Endurance – MALE) sınıfı taktik, stratejik ve özel görev İHA'lar genellikle askeri amaçlarla kullanılmaktadır. Ayrıca, özel görev İHA'lar uzay araştırmalarında da kullanılmaktadır.

Çizelge 3.1. EUROUVS İHA sınıflandırması [16, 17]

Kategori		Maksimum Kalkış Ağırlığı (kg)	Maksimum Uçuş Yüksekliği (m)	Havada Kalma/Dayanım Süresi (saat)	Veri Haberleşme Menzili (km)
Mikro/Mini İHA	Mikro	0.1	250	1	<10
	Mini	<30	150-300	<2	<10
Taktik İHA	Yakın Menzil	150	3000	2-4	10-30
	Kısa Menzil	200	3000	3-6	30-70
	Orta Menzil	150-500	3000-5000	6-10	70-200
	Uzun Menzil	-	5000	6-13	200-500
	Dayanımlı	500-1500	5000-8000	12-24	>500
	Orta İrtifa Uzun Havada Kalış (MALE)	1000-1500	5000-8000	24-48	>500
Stratejik İHA	Yüksek İrtifa Uzun Havada Kalış (HALE)	2500-12500	15000-20000	24-48	>2000
Özel Görev İHA	Öldürücü	250	3000-4000	3-4	300
	Tuzak	250	50-5000	<4	0-500
	Stratosferik	-	20000-30000	>48	>2000
	Ekzosferik	-	>30000	-	-

Ülkemizde son yıllarda askeri alanda İHA'lara yönelik yatırımlar artmıştır. Taktik MALE sınıfında TAI (Türk Havacılık ve Uzay Sanayii A.Ş.) tarafından ANKA, Baykar tarafından Bayraktar Taktik İHA ve Vestel tarafından Karayel insansız hava araçları üretilerek tüm testleri başarılı bir şekilde tamamlanmıştır. Dünya standartlarında yerli ve milli teknolojiler barındıran bu sistemler Türk Silahlı Kuvvetleri tarafından keşif, takip ve imha görevlerinde aktif olarak kullanılmaktadır.

3.2. İnsansız Hava Araçları Haberleşme Yöntemleri

İHA'ların kontrolünü sağlamak amacıyla çeşitli kablosuz haberleşme teknolojileri kullanılmaktadır. Kullanılan teknoloji, araçların faaliyet alanlarına göre değişiklik göstermektedir. Genellikle İHA'larda kullanılan kablosuz haberleşme teknolojileri aşağıdaki gibidir [16]:

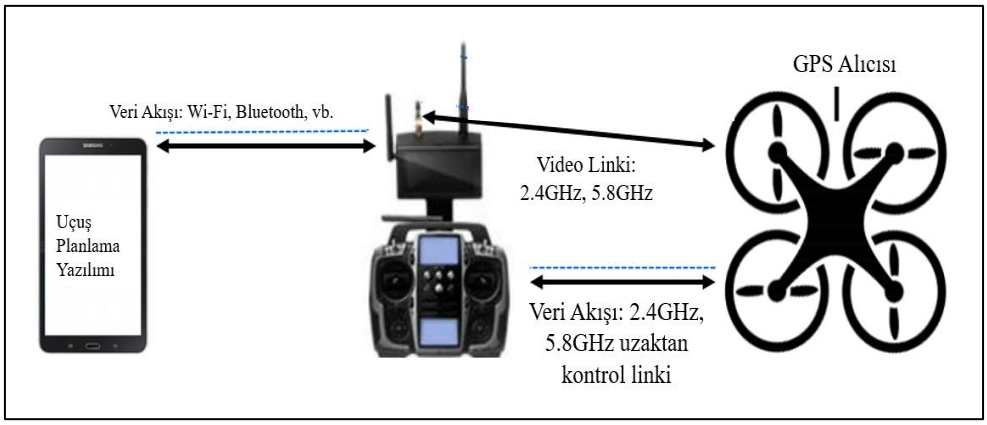
- Bluetooth
- Wi-Fi
- Radyo(RF)

- 3G/4G/LTE
- Uydu (Satellite)
- GPS

Bluetooth teknolojisinin kullanıldığı araçlar 20 metre civarında kısa bir menzile ve sınırlı uçuş süresine sahiptir. Bu araçlar genellikle eğlence amacıyla kullanılmaktadır. Wi-Fi teknolojisini kullanan araçlar da bluetooth teknolojisine benzer bir şekilde 50 metre civarında kısa bir menzile ve sınırlı uçuş süresine sahiptir. Yine aynı şekilde Wi-Fi haberleşmesi kullanan araçlar da eğlence ve hobi için tercih edilmektedir [16].

Radyo frekansları üzerinden haberleşen hava araçları genellikle 900MHz, 1.3GHz, 2.4GHz ve 5.8GHz frekanslarını kullanmaktadır. Ticari, hassas tarım, felaket kurtarma, video yayını, vb. amaçlarla kullanılan ve teknoloji marketlerinde en çok satılan insansız hava araçları genellikle 2.4GHz ve 5.8GHz frekanslarını kullanmaktadır. Bir frekans, aracı kontrol etmek için kullanılırken diğer frekans canlı video aktarımı için kullanılmaktadır. Üretici firmaların tecrübeleri, tek frekans üzerinden hem kontrol hem de video aktarımı yapıldığında çeşitli problemler yaşandığını göstermektedir. Radyo frekansı ile çalışan küçük hava araçları 2 kilometre menzile ulaşabilmektedir [16].

3G/4G/LTE teknolojisi, internet servis sağlayıcı alt yapısını kullanan uzun menzilli bir iletişim yöntemidir. İHA'ların kapasitesi ve uygun mobil taşıyıcı sinyallerin tespit edilmesine bağlı olarak maksimum menzil değişebilmektedir. Uydu haberleşmesi genellikle askeri amaçlı olarak kullanılan yüksek menzilli bir teknolojidir [16]. Otonom kontrol sağlamak için Amerika'da askeri kullanım amacıyla oluşturulmuş olan GPS (Global Positioning System) teknolojisi kullanılmaktadır. Keşif, gözetleme, takip ve saldırı görevlerinde askeri İHA'lar bu teknolojilerden aktif olarak yararlanmaktadır [1]. Şekil 3.2'de örnek bir insansız hava aracı haberleşme topolojisi sunulmaktadır.



Şekil 3.2. Örnek bir insansız hava aracı haberleşme topolojisi [18]

3.3. İnsansız Hava Araçlarına Yönelik Müdahale Yöntemleri

İHA'lar faydalı ya da kötü amaçlar için kullanılabilmektedir. Kötü amaçlarla kullanıldığı durumlarda, kişisel mahremiyet ve ulusal güvenlik açısından geniş bir yelpazede ihlâllere sebebiyet verilebilmektedir. İHA'larla birlikte özel hayatın gizliliği ile bireysel hak ve özgürlüklerin korunmasına yönelik geleneksel tedbirler yetersiz kalmıştır. Sosyal hayatın yanı sıra askeri ve casusluk amaçlarıyla kullanılan İHA'lar da başka ülkelere ait bilgilere keşif, gözetleme ve takip gibi faaliyetlerle ulaşarak devletlerarası krizlere yol açabilmektedir [16].

Kötü amaçlarla kullanılan İHA'lara karşı çeşitli müdahale yöntemleri geliştirilmiş ve geliştirilmeye devam etmektedir. Bu yöntemler aşağıda belirtilmektedir [16]:

- Pasif Önlemler
- Aktif Önlemler

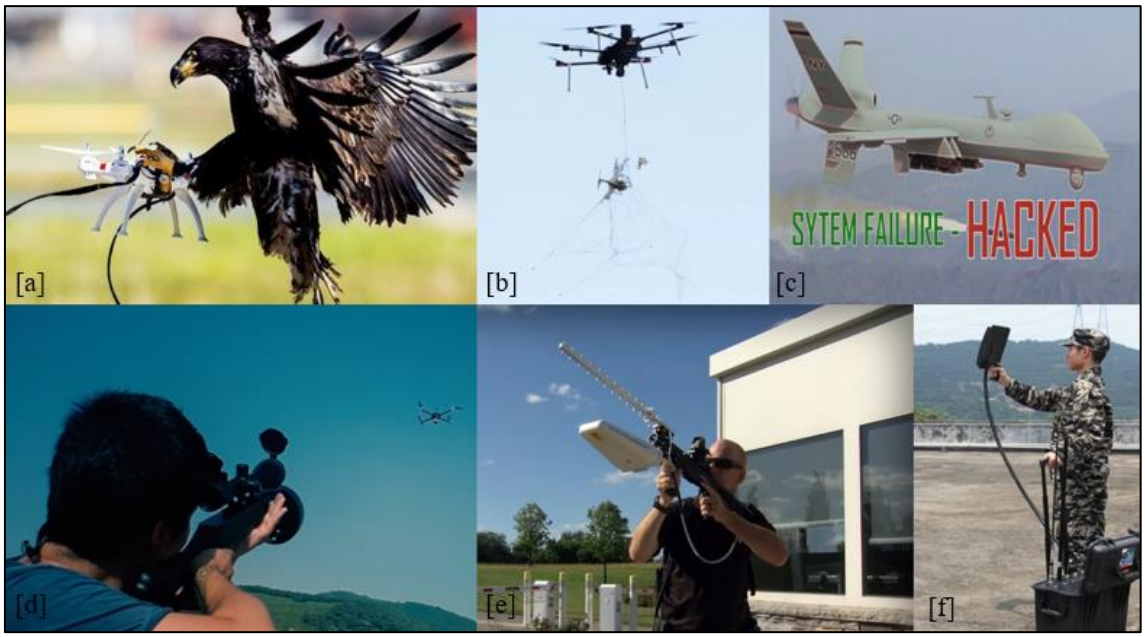
İHA'ların etki alanını kısıtlamaya yönelik dolaylı önlemler, pasif önlemler kategorisinde yer almaktadır. Kapıları otomatik kilitleme, görüntü kaydedilmesini engellemek için perdeleri kapatma, insanları uyararak güvenli alanlara yönlendirme gibi durumlar pasif önlemlere örnek verilebilmektedir [16].

Aktif önlemler direkt olarak bir İHA'nın işlevini kısmen veya tamamen kısıtlamaya yönelik girişimleri içermektedir. Belirtilen yöntemler aşağıda sunulmaktadır [16]:

- Müdahale İnsansız Hava Araçları
- Sinyal Engelleyici (Jammer)
- Ateşli Silahlar
- Elektromanyetik/Mikrodalga Işınlar
- Özel Yetiştirilmiş Yırtıcı Kuşlar
- Hekleme (hacking)

Şekil 3.3'te İHA'lara müdahale yöntemlerine ait görüntüler sunulmaktadır. Küçük boyutlardaki İHA'ların etkisiz hale getirilmesi için kullanılan yöntemlerden birisi de yırtıcı kuşlardır. Kartal gibi kuşlar eğitilerek doğal avlarına yaptıkları saldırıya benzer bir şekilde İHA'ları da avlayabilmektedir (Şekil 3.3a). Bu yöntem kısa vadede başarılı gibi görünse de silahlı hava araçlarıyla hayvanlar caydırılabilmektedir [16].

Müdahale hava araçları, yakın mesafeden hedeflenen İHA'yı etkisiz hale getirmek amacıyla ağ atmaktadır (Şekil 3.3b). Çok yetenekli pilot bulundurma, düşme riski ve güçlü araç bulundurma ihtiyaçları gibi dezavantajları bulunmaktadır [16].



Şekil 3.3. İnsansız hava araçlarına yönelik müdahale yöntemleri [16]

İHA’lar barındırdıkları siber güvenlik zafiyetleri vasıtasıyla da hedef alınabilmektedir (Şekil 3.3c). Heklemenin, diğer müdahale yöntemlerine göre maliyetsiz olması sebebiyle gelecekte en çok tercih edilecek yöntemler arasında olacağı değerlendirilmektedir [16].

Ateşli silahlar, İHA’lar karşısında zayıf etki alanına sahiptir (Şekil 3.3d). Son zamanlarda İHA’ların ucuz maliyetli olması ve araçlar arasında etkileşimli ağların kurulması gibi özellikler dikkate alındığında ateşli silahlar etkin bir çözüm olmamaktadır [16].

Ateşli silahlar gibi elektromanyetik/mikrodalga ışınları da zayıf etki alanına sahiptir (Şekil 3.3e). Radarlar tarafından tespit edilen İHA’ların kamera, uçuş kontrol bilgisayarı ve sensör gibi elektronik donanımlarını bozmak için kullanılmaktadır. Öte yandan bu ışınları kullanmak, özel izin gerektirebilmektedir [16].

Sinyal engelleyici (Jammer) kullanılarak İHA’ların GPS ve radyo bağlantısı engellenebilmekte ve etkisizleştirilebilmektedir (Şekil 3.3f). Engellenen İHA, sahip olduğu özelliklere göre başlangıç koordinatlarına geri dönme gibi eylemler gerçekleştirmektedir. Böylece saldırı yapan aracın faaliyetlerini engelleme ve saldırgan operatörün tespiti edilmesi gibi avantajları bulunmaktadır. Ancak, bölgedeki diğer Wi-Fi ve GPS gibi normal kablosuz yayınları etkileme, otonom uçan araçlarda etkisiz olma ve İHA’ları yerleşim yerleri üzerine düşürme gibi riskleri taşımaktadır [16].

4. İNSANSIZ HAVA ARAÇLARINDA SİBER GÜVENLİK

Kablosuz haberleşme teknolojileri İHA'lar tarafından aktif olarak kullanmaktadır. Ayrıca, İHA, yer kontrol istasyonu ve sensör gibi bileşenleri de bünyesinde barındırmaktadır. Bahse konu her bileşen/teknoloji birtakım tehdit ve saldırılara maruz kalabilmektedir [16].

4.1. İHA Sistemlerine Yönelik Başlıca Siber Tehditler

İnsansız hava araçlarının kullandığı teknolojiler birtakım tehditleri beraberinde getirmektedir. Çizelge 4.1'de İHA sistemlerine yönelik çeşitli tehdit/saldırı çeşitleri sunulmaktadır.

Çizelge 4.1. İHA sistemlerine yönelik başlıca siber tehditler [16,19]

Bileşen/Teknoloji	Tehdit/Saldırı
Uydu Haberleşmesi	Zayıf Şifreleme
	Trafik Sebebiyle Yaşanan Yoğunluk
	Erişilebilirliğe Yönelik Saldırılar(Sinyal Kesme, Hizmet Engelleme, vs.)
Diğer Radyo Haberleşme Bağlantıları	Gizliliği İfşa Edilmiş İHA'lar
	Gizli Dinleme
	Radyo Sinyali Kesme (Jamming) ve Hizmet Engelleme (DoS)
	Konum Gizliliği Saldırısı
İnsansız Hava Aracı	GPS Aldatmacası
	Fuzzing Saldırısı
	Ele Geçirme ve Etkisiz Hale Getirme
	Kazanç Ayarlama Saldırısı
Yer Kontrol İstasyonu	Zararlı Yazılım Enjeksiyonu
	Keylogger ve Diğer Veri Çıkarma Mekanizmaları
	Zayıf Kimlik Doğrulama
Komuta ve Kontrol Mesajları	Zayıf Mesaj Doğrulaması
	Kontrol Kanalı Sinyal Engelleme
Sensör/Algılayıcı	Sensör ve Çalıştırıcı Manipülasyonu
	Aldatmaca

Uydu haberleşmesi büyük mesafelerde kullanılan İHA'lar için olmazsa olmaz bir teknolojidir. Küresel konumlandırma sistemleri de uydu haberleşme teknolojisini

kullanmaktadır. Bu teknoloji; zayıf şifreleme, trafik sebebiyle yaşanan yoğunluk, sinyal kesme ve hizmet engelleme gibi erişilebilirliğe yönelik saldırılarla istismar edilebilmektedir [16,19].

Ayrıca, İHA'lar GPS aldatmacası ile farklı lokasyonlara yönlendirilmekte, yer kontrol istasyonunda bulunan sistemler zararlı yazılımlar ile kullanılamaz hale getirilmekte ve sensörler üzerindeki veriler manipüle edilebilmektedir. Öte yandan zararlı yazılımlar ile sistemlere ait gizli bilgiler de çıkartılabilmektedir [16,19].

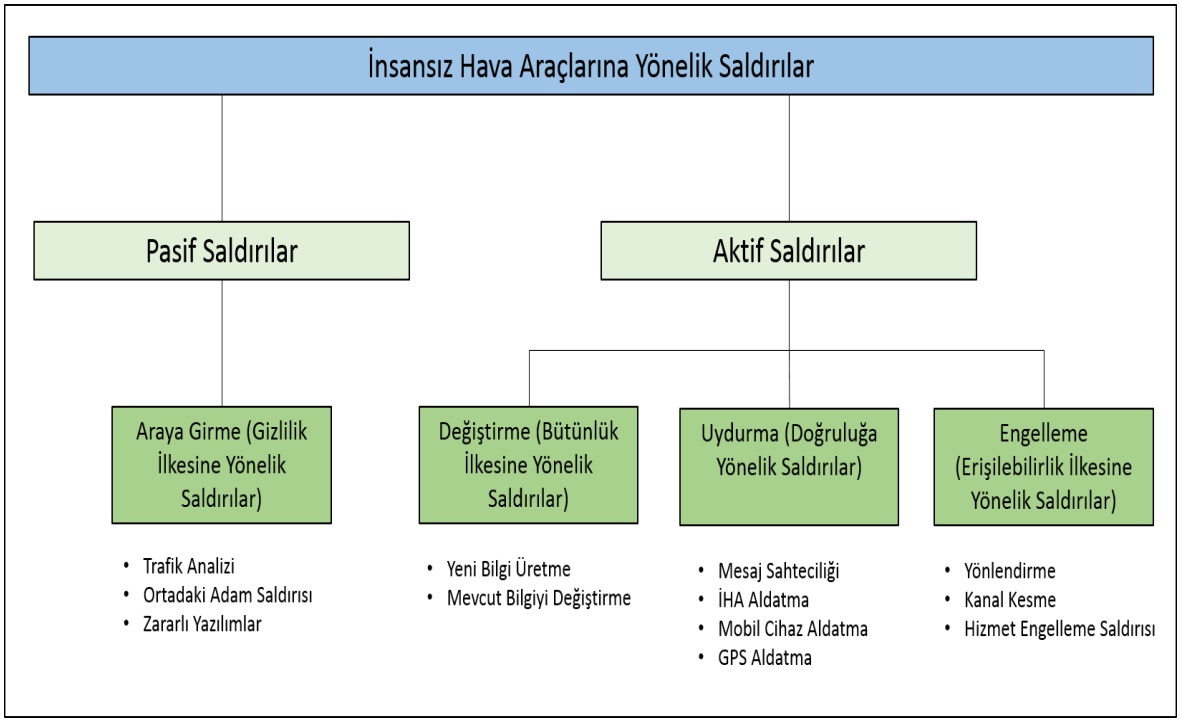
Özetle, yukarıda belirtilen bileşen/teknolojiler siber güvenliğin gizlilik, bütünlük ve erişilebilirlik ilkelerine zarar verebilecek çeşitli tehdit ve saldırılara maruz kalabilmektedir.

Doğal afetler veya sabotaj eylemleri sonucunda haberleşme kanallarının kesildiği acil durumlarda internet servis sağlayıcıları tarafından kurulan İHA destekli ağlar ile oluşabilecek mağduriyetler giderilebilmektedir. Böylece, bir İHA mobil istasyon, yönlendirme noktası ve uç terminal olarak da kullanılabilmektedir. İHA'lar bir baz istasyonu görevi alarak iletişim altyapısı oluşturmaktadır [16].

Benzer kritik kullanım amaçları göz önünde bulundurulduğunda İHA sistemlerinde bulunan donanım, yazılım ve haberleşme protokollerinde yer alan güvenlik zafiyetleri bir risk oluşturmaktadır [16].

4.2. İHA Sistemlerine Yönelik Siber Saldırılar ve Alınması Gereken Önlemler

İnsansız hava araçlarına aktif ve pasif olmak üzere iki sınıfta saldırılar gerçekleştirilmektedir. Trafik analizi ve ortadaki adam saldırısı pasif saldırılara örnek verilebilirken, aldatmaca, yönlendirme, kanal kesme ve hizmet engelleme saldırıları aktif saldırılara örnek gösterilebilmektedir. Şekil 4.1'de İHA sistemlerine yönelik saldırılar sunulmaktadır [16,20].



Şekil 4.1. İHA sistemlerine yönelik yapılan siber saldırılar [16,20]

Genel tehditler ve alınması gereken önlemler Çizelge 4.2'de sunulmaktadır. Siber güvenliğin gizlilik, bütünlük ve erişilebilirlik ilkeleri çeşitli saldırı yöntemleriyle zarara uğratılmaktadır.

Çizelge 4.2. Genel güvenlik tehditleri ve alınması gereken önlemler [16,20]

	Tehdit	Kategori	Önlem
1	Saldırganlar; hekleme, gizlice dinleme, kimlik aldatmacası ve katmanlar arası ağ saldırıları yoluyla bağlantıların güvenliğini tehlikeye atabilmektedir.	Gizlilik İlkesine Yönelik Saldırılar	Verilerin şifrelenmesi
2	Saldırganlar verilerin iletilmesi ve depolanması sırasında verileri değiştirebilmektedir.	Bütünlük İlkesine Yönelik Saldırılar	Mesaj doğrulama kodu gibi özet (hash) fonksiyonları
3	Saldırganlar haberleşme kanallarını engelleyebilmekte ve ağlara yönelik hizmet engelleme saldırıları gerçekleştirebilmektedir.	Erişilebilirlik İlkesine Yönelik Saldırılar	Güçlü kimlik doğrulama ile olay tespit ve raporlama mekanizmaları
4	Saldırganlar İHA sisteminde depolanan verilere yetkisiz erişim sağlayabilmekte ve verileri değiştirme yetkisi kazanabilmektedir.	Doğruluk İlkesine Yönelik Saldırılar	Verilere erişimde kimlik doğrulama ve şifreleme

Kötü niyetli kişiler/saldırganlar, Çizelge 4.2'de belirtilen yöntemlerle İHA sistemlerine tehdit oluşturmaktadır. Hekleme, gizlice dinleme, kimlik aldatmacası ve ağ saldırılarıyla verilerin açık metin olarak iletildiği durumlarda saldırganlar kolaylıkla verilere erişebilmektedir. Bu gibi durumlar için veriler şifrelenmelidir [16,20].

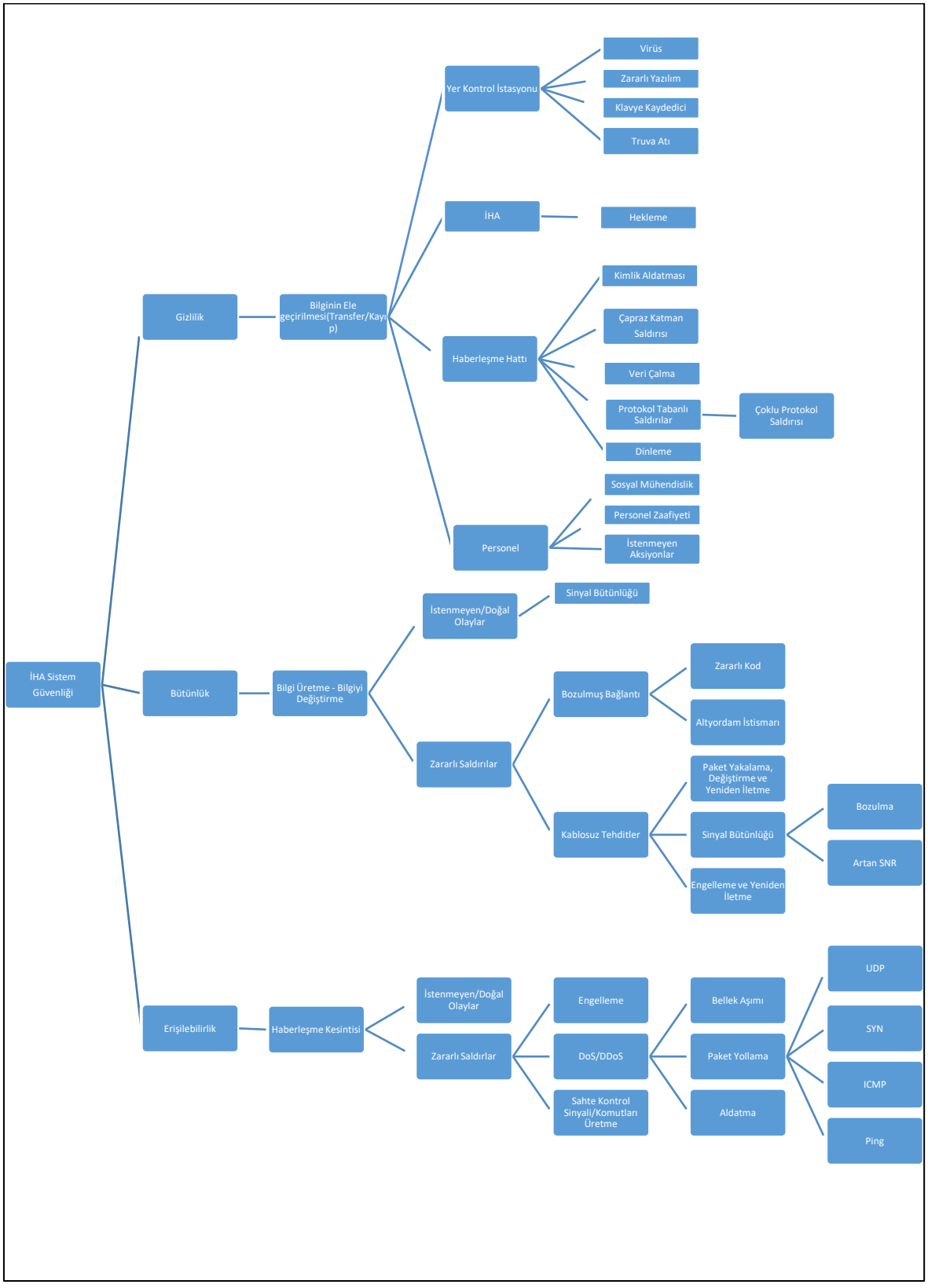
Verilerin taşınması ve barındırılması sırasında saldırganlar tarafından araya girme saldırılarıyla veriler değiştirilebilmektedir. Mesaj doğrulama kodu gibi özet (hash) fonksiyonları ile veri bütünlüğünün sağlanması için önlem alınabilmektedir [16,20].

Saldırganlar haberleşme kanallarını engelleyebilmekte ve ağlara yönelik hizmet engelleme saldırıları gerçekleştirebilmektedir. Güçlü kimlik doğrulama, olay izleme (monitoring) ve raporlama mekanizmaları ile belirtilen saldırılara karşı önlem alınabilmektedir [16,20].

İHA sistemlerinde depolanan verilere yetkisiz erişim sağlanabilmekte, veriler yetkisiz kişiler tarafından değiştirilebilmektedir. Verilere erişimde kimlik doğrulama ve şifreleme mekanizmaları kullanılmalıdır [16,20].

Siber tehditlere yönelik verilerin şifrelenmesi, mesaj doğrulama kodlarının kullanılması, olay tespit ve raporlama mekanizmaları ve verilere erişimde güçlü kimlik doğrulama gibi çeşitli tedbirlerin alınması gerekmektedir. Gerekli tedbirlerin alınması, saldırganlar için caydırıcı olmaktadır [16]. Ayrıca, Çizelge 4.3'te İHA sistem güvenliğini tehdit eden detaylı saldırı yöntemleri belirtilmektedir.

Çizelge 4.3. İHA sistem güvenliğini tehdit eden saldırılar [16,21]



İHA teknolojileri hızlı bir şekilde gelişmektedir. Bu gelişim sayesinde İHA'ların kullanım alanları giderek artmaktadır. Çizelge 4.3'ten de anlaşıldığı gibi teknoloji ile birlikte İHA sistemlerinin sürekli gelişmesi, çeşitli güvenlik zafiyetleri beraberinde getirmektedir [16].

Bütün bu gelişmelerin sonucunda İHA'larda siber güvenlik konusu büyük önem kazanmıştır. Literatürde bu alandaki çalışmaların az bulunması, henüz çok bakir bir alan olduğunu göstermektedir. 2011 yılında Amerikan Hava Kuvvetleri'ne ait İHA'nın İran tarafından ele geçirilmesinden sonra İranlı mühendisler tarafından GPS aldatmacası yönteminin kullandığı bilgisinin iletilmesiyle birlikte GPS aldatmacası konusunda çeşitli çalışmalar literatüre girmiştir [16].

İnsansız savaş uçakları, kamikaze ve sürü İHA'lar gibi teknolojilerin yapay zekâ, makine öğrenmesi, 5G ve nesnelerin interneti teknolojileriyle birlikte gelişmesiyle İHA'larda siber güvenlik konusu giderek önem kazanacaktır. İHA'ların bünyesinde barındırdığı her bileşen bir saldırı alanı oluşturmaktadır. Bu alanlara yönelik gerçekleştirilebilecek tüm tehdit ve saldırılar derinlemesine araştırma gerektirmektedir [16].

Ülkemizde yerli ve milli imkânlarla üretilen İHA'lara yönelik gerçekleştirebilecek saldırılar göz önüne alındığında, siber güvenlik açısından tüm bileşenlerin test edilmesi bir gereklilik olarak değerlendirilmelidir [16].

5. GPS VE DİĞER KÜRESEL KONUMLANDIRMA SİSTEMLERİ

Bu bölümde GPS ve diğer küresel konumlandırma sistemleri, GPS'in bilinen açıklıkları ve GPS aldatmacası tespit yöntemleri incelenmektedir.

5.1. GPS

GPS, Amerika Birleşik Devletleri Savunma Bakanlığı tarafından askeri kullanım amacıyla tasarlanan ve uzaya gönderilen 24 adet uydudan oluşan konumlandırma sistemidir. İlk olarak yalnızca askeri kullanımlara açık olan bu sistem, 1980 yılından itibaren sivil kullanıma da açılmıştır. Günümüzde ise konum, hız, zaman gibi bilgilere ihtiyaç duyulan gerek endüstriyel gerekse de eğlence amaçlı birçok uygulamada kullanılır duruma gelmiştir [2,22].

GPS sisteminin dışında Rusya tarafından geliştirilen GLONASS, Avrupa Birliği tarafından geliştirilen Galileo, Çin tarafından geliştirilen BeiDou ve Hindistan tarafından geliştirilen IRNSS konumlandırma sistemleri mevcuttur. Ancak GPS dışındaki sistemler, henüz yeterli olgunluk seviyelerine ulaşamadıkları için dünya genelinde GPS ağırlıklı olarak neredeyse her alanda kullanılmaktadır [4].

5.2. Glonass

Sovyetler Birliği döneminde devreye alınan ve Rusların askeri amaçlar için geliştirmiş olduğu konumlandırma sistemidir. 2008 yılında sivil kullanıma açılan söz konusu sistem, uydu ağının genişletilmesi sebebiyle küresel çapta kullanılan bir konumlandırma sistemine dönüşmüştür. GPS sistemi gibi 24 adet uydudan oluşmaktadır.

5.3. Galileo

Avrupa Birliği tarafından ABD'nin GPS ve Rusya'nın GLONASS sistemine alternatif olarak geliştirilen konumlandırma sistemidir. İlk uydusunun fırlatılışı 2005 yılında gerçekleşirken, 2019 yılı sonunda 27 aktif ve 3 yedek olmak üzere 30 uydu ile hizmet vermesi beklenmektedir.

5.4. Compass/BeiDou

Çin tarafından geliştirilen konumlandırma sistemidir. Toplamda 10 adet uydu ile 2013 yılında Çin'de kullanılmak üzere faaliyete geçmiştir. 2020 yılında 35 adet uydu ile küresel olarak hizmet vermesi beklenmektedir.

5.5. IRNSS

Hindistan tarafından geliştirilen konumlandırma sistemidir. 7 uydudan oluşan sistemin geliştirmeleri devam etmektedir.

5.6. GPS'in Güvenlik Açıklıkları ve Olası Etkileri

Teknolojinin hızla gelişmesinin bir sonucu olarak yaygın kullanıma sahip olan GPS sistemi maalesef sivil alanda, askeri alanda olduğu gibi yeterince güvenli değildir. Askeri uygulamalarda GPS verileri şifreli olarak iletilirken, sivil uygulamalarda veriler açık olarak iletilmektedir. Ayrıca söz konusu sistem, bozulmalara karşı çok hassastır. Çizelge 5.1'de GPS sisteminin bilinen açıklıkları ve olası etkileri sunulmaktadır.

Çizelge 5.1. GPS'in bilinen açıklıkları ve olası etkileri [23]

Bozulma Kaynağı	Günümüzde Gözlenen Örnekler	Oluşma Sıklığı	Engelleme Stratejileri
RF Paraziti	GPS Bandına yönelik Rahatsız Edici Kasıtsız Emisyonlar	Sık	Daha Güçlü GPS alıcı Teknolojisi ve Alternatif Zamanlama Kaynakları Kullanılması
Jamming Atağı	Yüksek Enerjili Jamming (Engelleme)	Nadir	Alternatif Zamanlama Kaynaklarının Kullanılması, Erteleme
GPS Aldatmacası	"In the wild" spoofing observed at DEF CON 23/24; GPS-SDR-Sim.	Nadir	Daha Güçlü GPS alıcı Teknolojisi, GPS Geliştirmesi, Alternatif Zamanlama Kaynakları Kullanılması
GPS Anomalileri	2016 UTC-offset error, January 2004 and July 2001 satellite clock failures.	Nadir	Alternatif Zamanlama Kaynakları Kullanılması
Lisanslı Bitişik Bant vericiler	Yok	N/A	Daha Güçlü GPS alıcı Teknolojisi ve Alternatif Zamanlama Kaynakları Kullanılması, Lisanslı Bitişik Bant Vericilerden Bant Dışı Bırakma Emisyonlarını Minimize Etmek
Çevresel Faktörler	GPS Anten Kurulumları, Çok Yollu Parazit, Troposferik Etkiler, İyonosferik Sintilasyon, Güneşli Hava Durumu.	Sık	Anten Kurulumu Yapan Teknisyenleri Eğitmek ve Alternatif Zamanlama Kaynakları Kullanılması

Gps aldatmacası, tespit edilmesinin zor olması sebebiyle diğer saldırı çeşitlerine göre daha etkili sonuçlar doğurmaktadır.

5.7. İnsansız Hava Araçlarına Yönelik GPS Aldatmacası Saldırıları

İnsansız hava araçlarına yönelik GPS aldatmacası saldırısı tespit yöntemleri, Bernal tarafından 2016 yılında yapılan çerçeve niteliğindeki çalışma neticesinde, tespit yöntemleri ve gereksinimler Çizelge 5.2'de özetlenmektedir.

Çizelge 5.2. GPS aldatmacası tespit yöntemleri özeti [4]

Yöntem	Açıklama	Şifreleme	Ağa Bağlı/Bağımsız	Tek veya Çoklu Anten	Katman	Gerekli Kapasite
Çoklu Anten Kullanılarak, Düşük Karmaşıklık Seviyesinde GPS Spoofing Engelleme Metodu	Aynı kaynaktan gelenlere boş değer atamak üzere, tüm sahte PRN kodlarının iletildiği yönü tahmin eder.	Hayır	Bağımsız	Çoklu	Sinyal İşleme	Birden Fazla Alıcı Anteni
Veri Biti Gecikme Savunması	Hedef alıcı, veri bit işareti değişikliklerini arayan C/A kod uzunluğundaki bit kilidini sürekli olarak izler	Hayır	Bağımsız	Tek	Veri Biti	C/A kod uzunluğundaki bit kilidini izler
İşaretli Sinyal Savunması	Birden fazla sinyali ayırt etmek için gerçek sinyali işaretleme	Hayır	Bağımsız	Tek	Sinyal İşleme	İşaretli gerçek GPS sinyalini filtreleme
Anten Tabanlı Ortak Tutum Tahmini	Gerçek GNSS ve spoofing sinyalleri arasında ayrım yapmak için tahmini varış yönünü kullanma	Hayır	Bağımsız	Çoklu	Veri Biti	Minyatürleştirilmiş anten dizisi
Korelatör Çıktı Dağılımı Analizi	Korelatör çıkış dağılımının, gerçek sinyalin dağıtımından önemli ölçüde sapıp sapmadığını tespit eder.	Hayır	Bağımsız	Tek	Sinyal İşleme	Korelatör çıktısının dağılımını izleme
Kod ve Taşıyıcı İzleme Seviyesinde Sahte GPS Sinyallerinin Tespiti	Spoofing saldırılarında meydana gelen sinyal kaldırması sırasında bozulmaları izler	Hayır	Bağımsız	Tek	Sinyal İşleme	Özel sinyal işleme kabiliyeti gerektirmektedir.
Alıcı Otonom Bütünlük İzleme (RAIM)	Sadece iki PRN olduğunda sahte sinyal algılar	Hayır	Bağımsız	Tek	Konum Çözümü ve Navigasyon Seviyesi	RAIM İmplementasyonu
Mutlak Güç İzlemesine Dayalı Sahtecilik Ayrımcılığı	2db'lik bir belirsizlikle, tipik ve maksimum olası değerler arasında mutlak sinyal gücünü izler	Hayır	Bağımsız	Tek	Sinyal İşleme	Alıcı mutlak alınan güç ve gürültü tabanını analiz edebilmelidir

Çizelge 5.2. (devam) GPS aldatmacası tespit yöntemleri özeti [4]

Ataletli Navigasyon Sistemi ile RAIM Kullanılarak GPS Spoofing Algılama	RAIM algoritması ile elde edilen GPS sahte ölçümleri ve ataletli navigasyon sistemi ölçümleri arasındaki tutarsızlıkları izler	Hayır	Bağımsız	Tek	Konum Çözümü ve Navigasyon Seviyesi	IMU sensörleri ve RAIM İmplementasyonu
İlişkili GPS Sinyal Gücü İzleme	Spoofing saldırıları sırasında meydana gelen sinyal gücündeki ani değişiklikleri izler	Hayır	Bağımsız	Tek	Sinyal İşleme	Sinyal Gücü İzleme
Alınan Her bir Uydu Sinyalinin Gücünü İzleme	Alınan her bir uydu sinyalinin gücünü İzler	Hayır	Bağımsız	Tek	Sinyal İşleme	Sinyal Gücü İzleme
Uydu Tanımlama Kodlarını ve Uydu Sinyallerinin Sayısını İzleme	Alınan uydu sinyallerinin sayısını ve SV ID kodlarını zaman içinde izleyerek, saldırı girişimlerini algılayabilir.	Hayır	Bağımsız	Tek	Sinyal İşleme	SN PRN İzleme
Zaman Aralıklarını Kontrol Etme	Her uydu sinyalinin edinimi arasındaki zaman aralığını kontrol eder	Hayır	Bağımsız	Tek	Sinyal İşleme	SV düzeltme zamanları arasındaki aralıkları izleme
Alıcı Hareketine Karşı Alınan Güç Değişimleri	Alıcı hareket halindeyken sinyal gücünde önemli ve anormal değişiklikler izlenir	Hayır	Bağımsız	Tek	Sinyal İşleme	Anten hareketi ve sinyal gücü izleme
L1/L2 Güç Seviyesi Karşılaştırması	L1 ve L2 bandındaki sinyal gücü farklılıklarını izler	Hayır	Bağımsız	Tek	Sinyal İşleme	Alıcı L1/L2 bandında çalışmalıdır
Çoklu Anten ile Spoofing Ayırt Etme	GPS korelatörleri, spoofer'ı bulmak için çok sayıda ışın çıkışına uygulanır	Hayır	Bağımsız	Çoklu	Sinyal İşleme	Çoklu alıcı anteni
PRN Kod ve Veri Bit Gecikmesi (TOA)	Spoofer veri biti sınırlarının gerçek olanlara göre mevcut olmayan zaman gecikmelerini kontrol etme	Hayır	Bağımsız	Tek	Sinyal İşleme	Varış zamanı analizi ve izleme
L1/L2 İlişkili Sinyal Gecikmesi (TOA)	L1 ve L2'nin bilinen korelasyon tepe farkını izler ve bu değerde ani değişiklikler arar	Hayır	Bağımsız	Tek	Sinyal İşleme	Alıcı L1/L2 bandında çalışırken varış zamanı analizi ve izleme

Çizelge 5.2. (devam) GPS aldatmacası tespit yöntemleri özeti [4]

Korelatör Çıktısının Dağılım Analizi	Korelatör çıktı dağılımındaki dalgalanmaları izler	Hayır	Bağımsız	Tek	Sinyal İşleme	Korelatör Çıktılarının Dağılım Analizi
Diğer GNSS'ler ile Tutarlılık Testi	Diğer GNSS PVT çözümlerini sürekli kontrol eder	Hayır	Bağımsız	Tek	Konum Çözümü ve Navigasyon Seviyesi	Çoklu GNNS alıcı donanımı
Diğer Konumlandırma Teknolojileri ile Tutarlılık Testi	Mobil veya Wi-Fi internet üzerinden gözlemlenen konum teknolojisi ile pozisyon çözümünün karşılaştırılması	Hayır	Bağımsız	Tek	Konum Çözümü ve Navigasyon Seviyesi	İnternet Bağlantısı
Diğer Teknolojiler ile Tutarlılık Testi	Üçüncü parti kaynaklar ile GPS veri bütünlüğünün karşılaştırılması (efemeris,almanac,time)	Hayır	Ağa Bağlı	Tek	Konum Çözümü ve Navigasyon Seviyesi	İnternet Bağlantısı
Farklı Sensörler ile Tutarlılık Testi	IMU, pusula veya statik ölçüm araçları üzerinden alınan verilerin analiz edilmesi ve karşılaştırılması	Hayır	Ağa Bağlı	Tek	Konum Çözümü ve Navigasyon Seviyesi	IMU, pusula veya statik ölçüm araçları
L1C Üzerindeki Yayılmış-Spektrum Güvenlik Kodları Temelli Savunma	Navigasyon mesajında yayılmış-spektrum güvenlik kodları tarafından üretilen dijital anahtarların taşınması	Evet	Bağımsız	Tek	Sinyal İşleme	GPS IS içinde modifikasyon: L1C veri kanalı dağıtım kodu
L1C, L2C veya L5(NMA) Üzerindeki Konum Mesajı Doğrulaması Temelli Savunma	GPS sivil navigasyon mesajına açık anahtar dijital imzalarının eklenmesi	Evet	Bağımsız	Tek	Sinyal İşleme	GPS IS içinde modifikasyon: 2 yeni CNAV mesajı
Alınan Efemeris Verisi ile Tutarlılık Testi	Farklı uyduların çıkarılan efemeris verileri arasındaki tutarsızlıklar	Hayır	Bağımsız	Tek	Veri Biti	İzleme ve efemeris karşılaştırması
GPS Saati Tutarlılık Testi	Farklı uyduların alınan zamanlar arasındaki tutarsızlıklar	Hayır	Bağımsız	Tek	Veri Biti	İzleme ve zaman karşılaştırması
Otomatik Kazanç Kontrolü ile Sahte Sinyalleri Yakalama	Sinyal girişiminin varlığını algılamak için Otomatik Kazanım Kontrol değerlerinde ani değişiklikleri izler	Hayır	Bağımsız	Tek	Sinyal İşleme	AGC izleme

Çizelge 5.2. (devam) GPS aldatmacası tespit yöntemleri özeti [4]

GPS PVT Çözümü ile Veri Tutarlılığı Testi	PVT çözümünde normal ve tahmin edilen davranışları izler	Hayır	Bağımsız	Tek	Konum Çözümü ve Navigasyon Seviyesi	PVT izleme

Yukarıda da belirtildiği üzere GPS aldatmacası tespit yöntemleri; tek veya çoklu anten ihtiyacı, uygulama katmanı ve gerekli kapasitelere göre sınıflandırılmıştır. Uygulamalar incelendiğinde büyük bir çoğunluğunun sinyal işleme metodolojisini kullandığı görülmektedir. Bunun dışında veri biti, konum çözümü ve navigasyon seviyesinde yöntemler geliştirilmiştir.

Sinyal işleme seviyesinde;

- Sinyal gecikmeleri,
- Sinyal gücü izlemeleri,
- Zaman aralıklarının kontrol edilmesi,
- Çoklu anten ile aldatmaca tespiti,
- Konum mesajı doğrulaması,
- Kazanç kontrolü metotları

Veri biti seviyesinde;

- Veri biti gecikmesi,
- Anten tabanlı ortak tutum tahmini,
- Alınan efemeris verisi ile tutarlılık testi
- GPS saati ile tutarlılık testi

Konum çözümü ve navigasyon seviyesinde ise;

- Diğer küresel konumlandırma sistemleri ile tutarlılık testi,
- Farklı sensörler ile tutarlılık testi

gibi yöntemler dikkat çekici bulunmaktadır.

6. İHA'LARDA GPS ALDATMACASI TESPİT UYGULAMASI

İHA'lar, GPS aldatmacası saldırılarıyla ele geçirilerek veya düşürülerek maddi kayıplara sebebiyet verilebilmektedir. Literatürdeki GPS aldatmacası tespit çalışmaları incelendiğinde sinyal işleme, veri biti, pozisyon ve navigasyon çözümü katmanlarında çalışmalar gerçekleştirildiği gözlemlenmektedir.

Uygulamada, İHA üzerindeki mevcut bileşenlerin dışında herhangi bir ekstra donanıma ihtiyaç duymamasından ve yer istasyonu üzerinden hızlı bir şekilde analiz kabiliyetine sahip olmasından dolayı pozisyon ve navigasyon çözümü katmanında çalışmalar gerçekleştirilmiştir.

Pozisyon ve navigasyon çözümü seviyesinde birden fazla GPS aldatmacası tespit yöntemi kullanılarak etkin bir sistem tasarlanması amaçlanmıştır. Bu tezde Ataletsel Ölçüm Birimi (AÖB) sensör verileri ve diğer küresel konumlandırma sistemleri verileri üzerinden sağlanan konum verileri karşılaştırılarak hibrit bir analiz yöntemi uygulanmıştır.

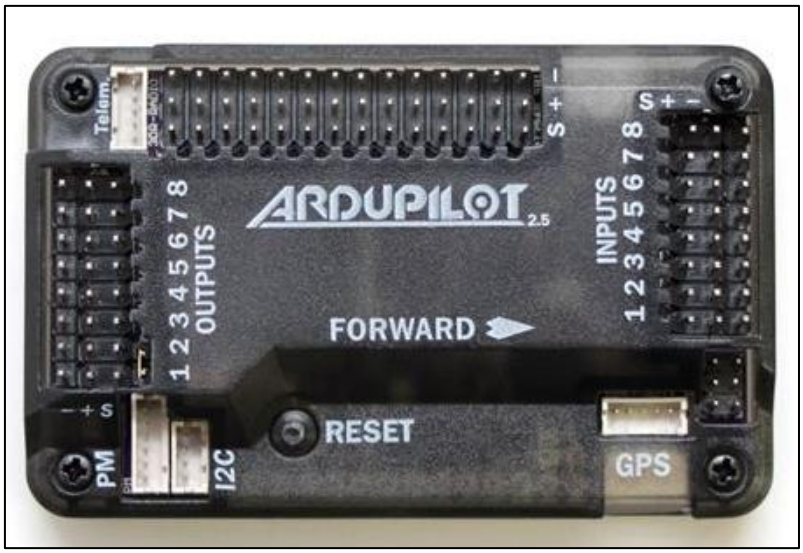
6.1. Uygulamada Kullanılan Donanımlar

Uygulamada birçok farklı donanımlarla uyum içerisinde çalışması amacıyla İHA tasarlanmıştır. "Quadrotor" olarak adlandırılan dört motora ve pervaneye sahip bir helikopter yapılmıştır. Ayrıca, quadrotor'da kullanılan donanımların açık kaynak kodlu olması tercih edilmiştir. Şekil 6.1'de tasarlanan İHA'ya ait görüntü sunulmaktadır.

Şekil 6.1. İnsansız hava aracı-quadrotor

6.1.1. ArduPilot mega (APM)

Ardupilot, Arduino temelli kontrol kartıdır. Genellikle mikro ve mini İHA grubunda kullanılan bu kart ile hava araçları otonom uçuş özelliği kazanabilmektedir. Kart üzerinde "ATmega2560" mikro kontrolcü bulunmaktadır. Ayrıca, ivmeölçer, barometre, manyetometre ve jiroskop gibi sensörler kart üzerinde mevcuttur. Şekil 6.2'de karta ait görüntü sunulmaktadır.



Şekil 6.2. ArduPilot mega (APM) [24]

Kart üzerinde ayrıca telemetri, GPS ve güç modülü gibi harici bağlantı noktaları bulunmaktadır. Birçok yer istasyonu ve uçuş kontrol yazılımları desteklenmektedir.

6.1.2. Telemetri modülü

İHA havadayken yer istasyonu ile haberleşmesini sağlayan modüldür. Alıcı ve verici ikilisinden oluşmaktadır. 915 MHz frekansında faaliyet göstermektedir. 1.5 kilometre civarında menzile sahiptir. Şekil 6.3'te telemetri modülüne ait görüntü sunulmaktadır.

Şekil 6.3. Telemetri modülü

6.1.3. GPS modülü

GPS modülü, hava aracının, belirtilen konumlara ulaşmasını, otonom uçuş gerçekleştirmesini ve aracın kalkış gerçekleştirdiği konuma geri dönmesini sağlamaktadır. Şekil 6.4'te GPS modülüne ait görüntü sunulmaktadır.

Şekil 6.4. GPS modülü

Genellikle hassas konum gerektiren uygulamalarda tercih edilen bu modülün üzerinde GPS ile birlikte GLONASS desteği bulunmaktadır [25].

6.1.4. RC kumanda

İHA'yı uzaktan kontrol etmeyi sağlayan 6 kanallı kumandadır. Led ekranı sayesinde direkt kumanda üzerinden İHA kalibrasyonları yapılabilmektedir. Şekil 6.5'te RC kumandaya ait görüntü sunulmaktadır.

Şekil 6.5. RC kumanda

Ayrıca, İHA üzerinde kontrol kartına bağlı bir alıcısı bulunmaktadır. Otonom uçuşların dışında büyük öneme sahiptir.

6.2. Uygulamada Kullanılan Yazılımlar / Programlar

GPS aldatmacası tespitinde yer kontrol istasyonu uygulaması olan Mission Planner ve nesne tabanlı kodlamalara imkân sağlayan Python programlama dili kullanılmıştır. Mission Planner uygulaması, Python programlama dili ile uyumludur. Python ile yazılmış kodlar Mission Planner uygulamasına aktarılarak çalıştırılabilmektedir.

6.2.1. Mission Planner uygulaması

Mission Planner, ArduPilot için tasarlanmış açık kaynak kodlu bir yer kontrol istasyonu uygulamasıdır. Şuan çoğu işletim sistemi tarafından desteklenmektedir. Söz konusu uygulamanın bazı önemli özellikleri aşağıdaki gibidir [26]:

- Otomatik görev oluşturma, kaydetme ve yükleme,
- Harita üzerinden görsel olarak görev yönetme,
- Görev loglarını indirme ve analiz etme,

- Uygun bir telemetri donanımıyla birlikte uzaktan araç durumunu izleme,
- Telemetri loglarını kaydetme ve analiz etme

Şekil 6.6'da Mission Planner uygulamasına ait ekran görüntüsü sunulmaktadır.

Şekil 6.6. Mission Planner uygulaması arayüzü [26]

Arayüzdeki "Script" sekmesi altında Python programlama dilinde yazılmış kodlar uygulama üzerinde çalıştırılabilmektedir. Bu özellik GPS aldatmacası tespit yöntemlerinde kullanılmıştır.

6.2.2. MAVLink protokolü

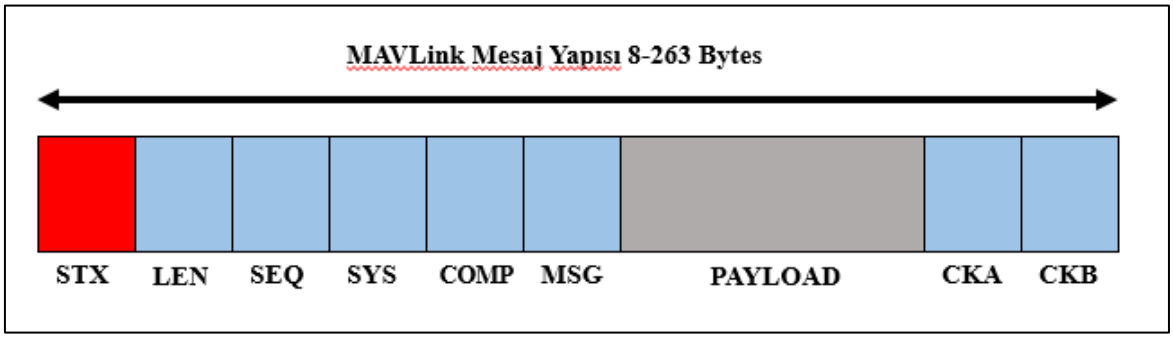
MAVLink (Micro Air Vehicle Link), ilk olarak 2009 yılının başında Lorenz Meier tarafından yayımlanan ve küçük insansız hava araçları ile yer istasyonları arasında iletişim kurmak için kullanılan mesaj tabanlı bir iletişim protokoldür [27].

Günümüzde binlerce geliştirici tarafından kullanılmaktadır. Ardupilot gibi otomatik pilot uygulamalarında tercih edilmektedir. Mission Planner ve İHA arasındaki haberleşme bu protokol ile gerçekleştirilmektedir. MAVLink protokolünde iletişim, İnsansız hava aracı ile yer kontrol istasyonu/kumanda arasında mesaj başlıkları olarak iki yönlü sağlanmaktadır.

Yer kontrol istasyonundan/kumandadan insansız hava aracına görev komutları gönderilmektedir. İnsansız hava aracı ise sensör verileri ve güncel konum dâhil olmak üzere bilgilerini yer kontrol istasyonuna iletmektedir.

MAVLink mesajları teknolojiye bağımsız olarak Wi-Fi, 900MHz radyo, vb. gibi neredeyse her bağlantı üzerinden gönderilebilmektedir. Mesajların teslim edilme garantisi bulunmamaktadır; bu, yer istasyonlarının veya yardımcı bilgisayarların bir komutun yürütülüp yürütülmediğini belirlemek için sık sık araç durumunu kontrol etmesi gerektiği anlamına gelmektedir [28].

MAVLink protokolüne ait mesaj yapısı Şekil 6.7'de ve mesaj yapısındaki değerlerin açıklamaları Çizelge 6.1'de sunulmaktadır.



Şekil 6.7. MAVLink mesaj yapısı [29]

Çizelge 6.1. MAVLink mesaj yapısı içerikleri [29]

Byte İndeksi	İçerik	Değer	Açıklama
0	Paket Başlama İşareti (STX)	0xFE	Yeni bir paketin başlangıcını içermektedir.
1	Yük/Veri Uzunluğu (LEN)	0 - 255	Yükün / Verinin uzunluğunu içermektedir.
2	Paket Sırası (SEQ)	0 - 255	Paket kaybını önlemek için paket iletim sırasını içermektedir.
3	Sistem ID (Kimlik)	1 - 255	Gönderen Sistem ID: aynı ağ üzerinde birden fazla platform belirlemeye izin vermektedir.
4	Bileşen ID	0 - 255	Bileşen ID: aynı platform üzerinde birden fazla bileşen belirlemeye izin vermektedir.
5	Mesaj ID	0 - 255	Mesaj ID: Yükün ne anlama geldiğini ve nasıl çözüleceğini belirtmektedir.
6 - (n+6)	Veri (Yük)	0 - 255 (Byte)	Mesaj Verisi: mesaj ID'sine bağlıdır.
(n+7) - (n+8)	Sağlama (CKA ve CKB)	1 - (n+6) byte ITU X.25/SAE AS-4 hash'i: Mesaj alanlarından hesaplanan MAVLINK_CRC_EXTRA parametresini içermektedir.	

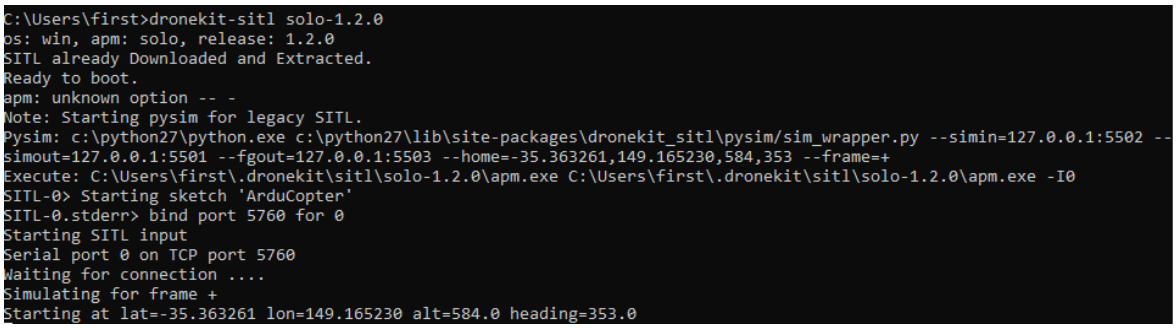
MAVLink protokolünün; MAVLink 1,0 ve MAVLink 2,0 olmak üzere iki sürümü bulunmaktadır. Son sürümü daha fazla esneklik ve güvenlik sağlamak amacıyla geliştirilmiştir. Şuan protokolün yönetimi “Dronecode” ve “The Linux Foundation” projeleri tarafından sağlanmaktadır.

6.2.3. Python programlama dili

Python nesne tabanlı programlamayı destekleyen, gelişmiş, genel amaçlı bir programlama dilidir. Neredeyse bütün işletim sistemleri tarafından desteklenmektedir. Diğer programlama dillerinin aksine öğrenmesi kolay ve derlenmeden çalışabilmektedir. Günümüzde artık büyük şirketler de dâhil olmak üzere kurumsal ortamlarda yaygın olarak kullanılmaktadır. Belirtilen özelliklerinden dolayı bu uygulamada Python programlama dili kullanılmıştır.

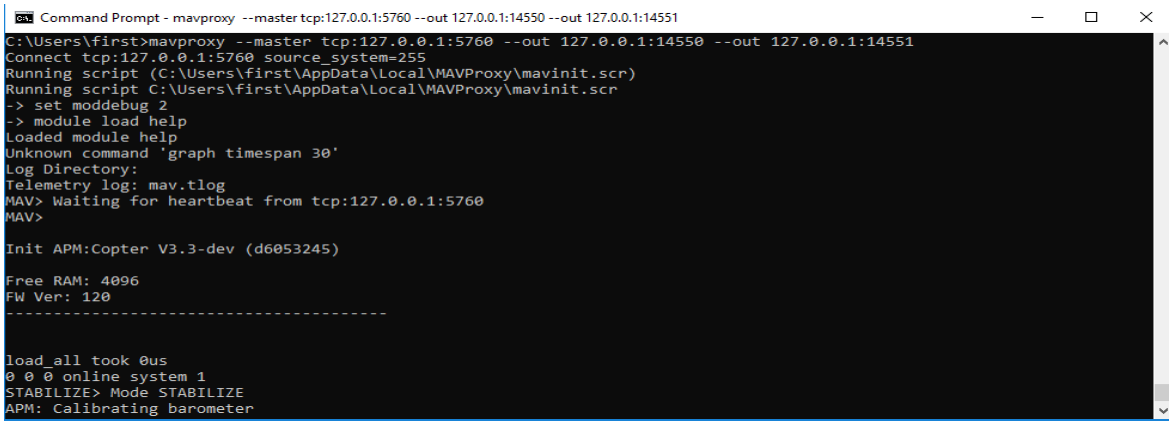
6.3. Test Ortamı Kurulumu

İHA'larda GPS aldatmacası tespiti çalışmaları için test simülasyonu oluşturulmuştur. Öncelikle Mission Planner'da kullanılmak üzere planlanan İHA simülatörü için Drone Kit-stil paketi kurulmuştur. Bu paket üzerinde solo-1.2.0, Rover-2.5.0 ve copter-3.3 gibi araçlar mevcuttur. Şekil 6.8'de simülatörün başlatılması sunulmaktadır.



Şekil 6.8. Simülatörün başlatılması

Ayrıca, yer istasyonu ile araç arasında bağlantı kurulmasını sağlayan MAVproxy uygulaması kurulmuştur. MAVproxy uygulaması, dronekil-sitl ve yer istasyonu (Mission Planner) arasında MAVLink protokolü üzerinden bağlantı kurulmasını sağlamaktadır. Bu özellik, çeşitli kodlar geliştirilerek arayüz üzerinden test edilmesine olanak sağlamaktadır. Şekil 6.9'da MAVproxy uygulamasının başlatılması sunulmaktadır.



Şekil 6.9. MAVproxy uygulamasının başlatılması

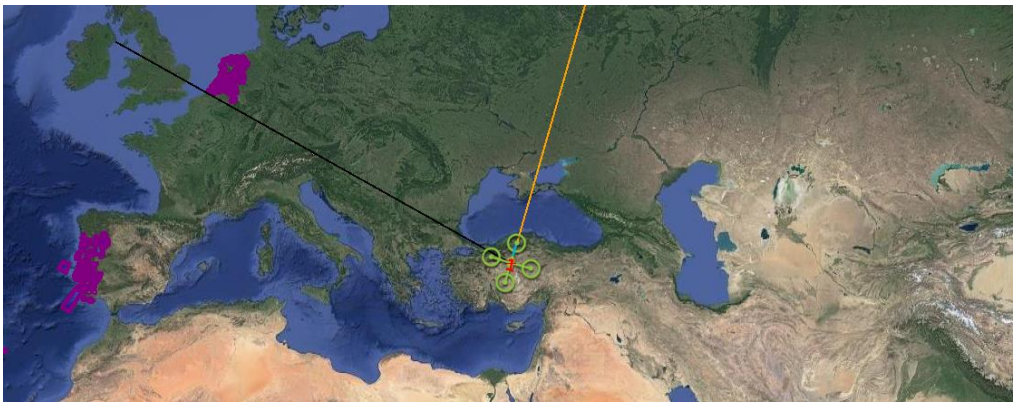
Mission Planner'da user datagram protokolü (UDP) üzerinden 14551 portuna bağlantı sağlanarak test ortamı hazır hale getirilmiştir.

6.4. İHA'dan Verilerin Okunması

GPS aldatmacası tespit çalışmalarında İHA üzerinden anlık verilerin elde edilmesi büyük önem taşımaktadır. İlk olarak İHA'ya telemetri modülü üzerinden uzaktan bağlantı gerçekleştirilmiştir. Mission Planner uygulaması ile gerçekleştirilen bağlantı sonucunda hava aracından elde edilen bazı anlık bilgiler Şekil 6.10'da sunulmaktadır.

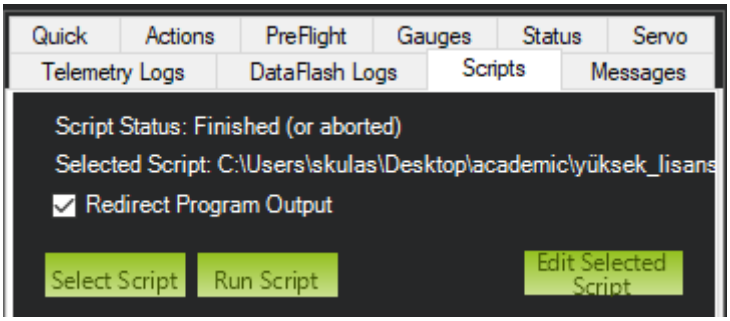
Şekil 6.10. Mission Planner – Sensör verileri ekranı

Ayrıca, Mission Planner uygulamasında İHA'nın güncel konum bilgisi Şekil 6.11'de görülmektedir.



Şekil 6.11. Mission Planner – Harita üzerinde İHA'nın mevcut konumu

Mission Planner uygulaması Python programlama diliyle uyumlu çalışmaktadır. Uygulama arayüzündeki “Scripts” sekmesinde Şekil 6.12’de gösterildiği gibi kodlar çalıştırılmaktadır. Kodların çıktısı hızlı bir şekilde çalışmaktadır.



Şekil 6.12. Mission Planner – Betik çalıştırma ekranı

Öncelikle İHA üzerindeki AÖB sensörü ve GPS modülü üzerindeki veriler okunmaktadır. Şekil 6.13’te belirtilen Python kodu ile birer saniye aralıklarla enlem, boylam, yükseklik, uydu sayısı, ivme ve rüzgâr hızı gibi çeşitli veriler çekilmektedir. Elde edilen çıktılar “getvalues.txt” isimli dosyaya yazdırılmaktadır.

```
# -*- coding: utf-8 -*-
import clr
import json
from time import sleep
clr.AddReference("MissionPlanner")
while True:
    print 'start'
    dosya = open("getvalues.txt","w")
    veri_dict = dict()
    veri_dict["altitude"] = cs.alt
    veri_dict["latitude"] = cs.lat
    veri_dict["longitude"] = cs.lng
    veri_dict["gpsstatus"] = cs.gpsstatus
    veri_dict["gpshdop"] = cs.gpshdop
    veri_dict["satellite_count"] = cs.satcount
    veri_dict["airspeed"] = cs.airspeed
    veri_dict["targetairspeed"] = cs.targetairspeed
    veri_dict["verticalspeed"] = cs.verticalspeed
    veri_dict["wind_direction"] = cs.wind_dir
    veri_dict["wind_welocity"] = cs.wind_vel
    veri_dict["accleration"] = [cs.ax, cs.ay ,cs.az]
    veri_dict["gyro"] = [cs.gx, cs.gy, cs.gz]
    veri_dict["traveled_dist"] = cs.distTraveled
    veri_dict["time_in_air"] = cs.timeInAir
    dosya.write(str(veri_dict))
    dosya.close()
    sleep(1)
    print 'finish'
```

Şekil 6.13. Sensör verilerini okuyan Python kodu

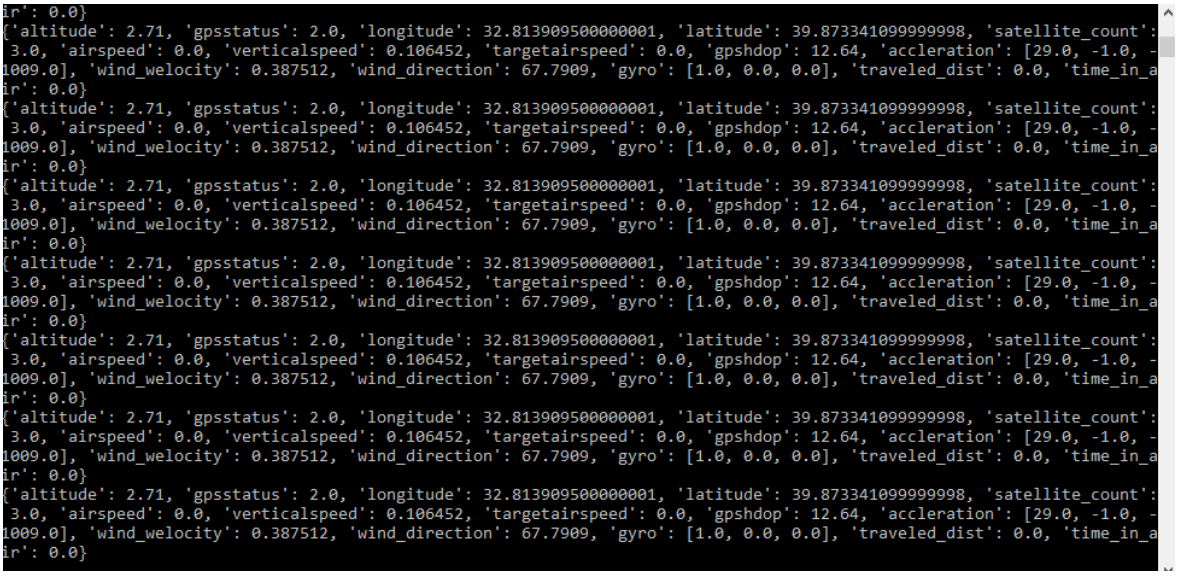
Yukarıda belirtilen kod çalıştırıldıktan sonra anlık olarak ekrana yazdırmak için Şekil 6.14'te belirtilen kod parçası kullanılabilmektedir.

```
import time
while True:
        x = open('getvalues.txt','r')
        for i in x:
                print(i)
        x.close()
        time.sleep(1)
```

Şekil 6.14. Sensör verilerini ekrana yazdıran Python kodu

Sonuç olarak İHA üzerindeki veriler anlık olarak okunarak komut satırı ekranına yazdırılmaktadır. Şekil 6.15'te anlık sensör verileri sunulmaktadır. Anlık sensör verileri işlenmek üzere bir metin dosyasında ve web sunucusunda sürekli olarak tutulmaktadır. Özellikle hız ve zaman verileri ile GPS konum bilgileri aldatmaca tespiti için büyük önem

taşımaktadır. Hız ve zaman bilgisinden elde edilen mevcut ve muhtemel konumlar hesaplanmaktadır. Eğer belirtilen aralığın dışına çıkılmış ise aldatmaca olma olasılığı artmaktadır. GPS konum bilgisi ve diğer GNSS sistemi verileri karşılaştırılarak aldatmaca tespiti yapılmaktadır.



Şekil 6.15. Anlık sensör verileri

6.5. AÖB Verileri ile GPS Verilerindeki Anomalilerin İzlenmesi

İHA'ların sahip olduğu hız, mesafe, yön, zaman gibi veriler ile harita üzerinde mantıklı çıkarım yapılarak konum tespiti yapılması "Dead Reckoning" olarak adlandırılmaktadır. Belirli bir zamanda konumu kesin olarak bilinen bir hava aracının sonraki konumunun hesaplanmasına imkân sunulmaktadır.

Mission Planner'da AHRS_GPS_USE parametresi "0" olarak ayarlandığında konumlandırma için GPS yerine Dead Reckoning kullanılmaktadır. Mission Planner'ın son sürümü de dâhil olmak üzere çeşitli sürümlerinde gerçekleştirilen analiz çalışmaları neticesinde, bu özelliğin düzgün olarak çalışmadığı gözlemlenmiştir. Bu çalışmada, daha doğruya yakın sonuçlar vermesinden dolayı Thaddeus Vincenty tarafından geliştirilen ve dünya üzerindeki iki koordinat arasındaki mesafeyi bulmak için iteratif işlemler kullanılmıştır [30].

Öncelikle GPS aldatmacası saldırılarını tespit edebilmek amacıyla belirli bir uçuş rotası oluşturulmuştur. Şekil 6.16'da planlanan uçuş rotası sunulmaktadır.

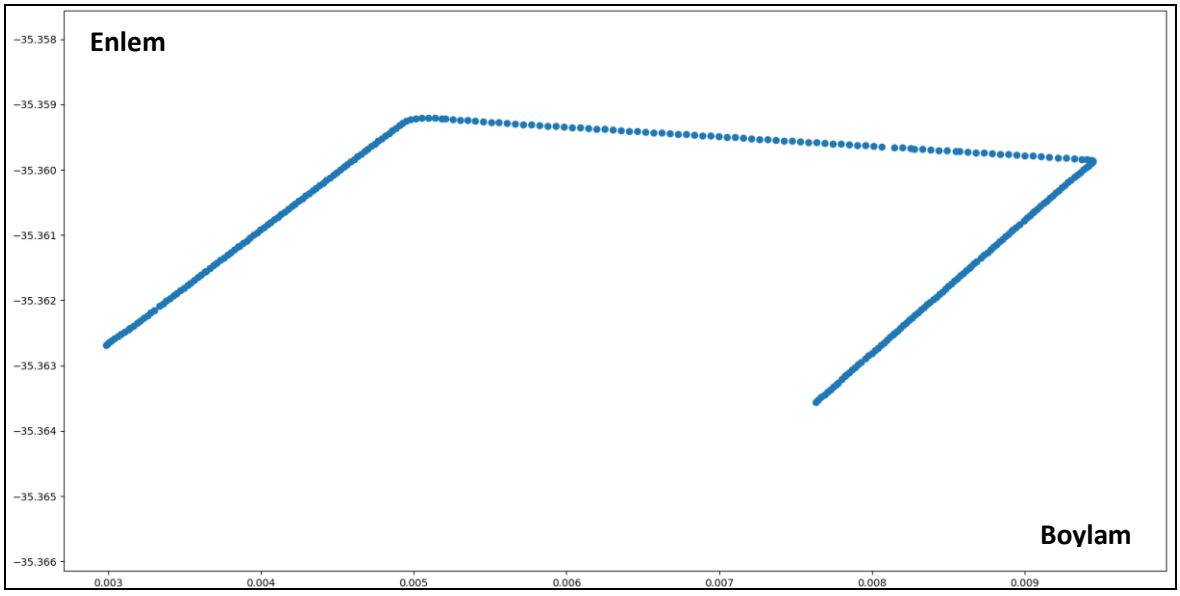
Şekil 6.16. Planlanan uçuş rotası

Uçuş rotası tamamlanarak Şekil 6.17'de sunulan Python betiği ile GPS üzerinden alınan enlem, boylam, kuzeyle yapılan açı ve bir saniye aralıklı şekilde zaman bilgisi toplanarak, .csv uzantılı olarak kaydedilmiştir.

```
# -*- coding: utf-8 -*-
import clr
import csv
import json
from time import sleep
clr.AddReference("MissionPlanner")
print 'helo'
with open('C:\Users\\first\Desktop\\fligtdata.csv', 'wb') as csvfile:
    spamwriter = csv.writer(csvfile, delimiter=',')
    spamwriter.writerow(['lat', 'lng', 'groundcourse', 'groundspeed', 'timeInAir'])
    saniye = 0
    while saniye<=30000:
        spamwriter.writerow([cs.lat, cs.lng, cs.groundcourse, cs.groundspeed, saniye])
        sleep(1)
        saniye = saniye + 1
        csvfile.flush()
```

Şekil 6.17. Veri toplayan Python betiği

Daha sonra Şekil 6.18'deki gibi rotaya göre GPS'ten elde edilen enlem ve boylam bilgilerinden konumlar çizdirilmiştir.



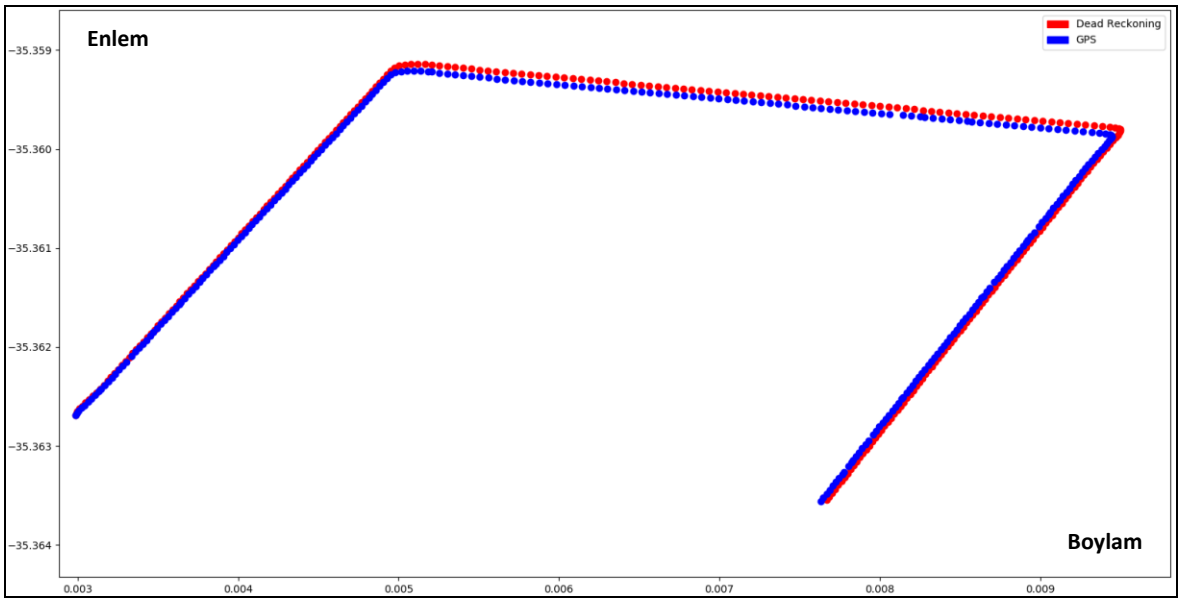
Şekil 6.18. Planlanan rota GPS konum verileri

Dead reckoning algoritmalarında belirtildiği gibi bir noktadaki kesin konumu, hızı, açısı ve zamanı (1 saniye aralıklı) bilinen verilerden hareketle, Vincenty işlemleri kullanılmıştır. Şekil 6.19'daki Python betiğiyle ilk noktadaki GPS verisi üzerinden gerekli hesaplamalar yapılmıştır.

```
dead_lat=[]
dead_long=[]
duz_long = []
duz_lat = []


onceki_lat = 0
onceki_long = 0
with open('gps_date_5.csv') as csvfile:
    reader = csv.DictReader(csvfile)
    for index, row in enumerate(reader):
        duz_lat.append(row['lat'])
        duz_long.append(row['lng'])
        if index == 0:
            onceki_lat = float(row['lat'])
            onceki_long = float(row['lng'])
            dead_lat.append(onceki_lat)
            dead_long.append(onceki_long)
        hiz = float(row['groundspeed'])
        aci = float(row['groundcourse'])
        distance = hiz / 1000
        origin = geopy.Point(onceki_lat, onceki_long)
        destination = VincentyDistance(kilometers=distance).destination(origin, aci)
        yeni_lat = destination.latitude
        yeni_long = destination.longitude
        #print(str(hiz), " ", str(aci), " ", str(onceki_lat), " ", str(onceki_long), " ", str(yeni_lat), " ", str(yeni_long))

        onceki_lat = yeni_lat
        onceki_long = yeni_long

        dead_lat.append(yeni_lat)
        dead_long.append(yeni_long)


dead_lat = [float(x) for x in dead_lat]
dead_long = [float(x) for x in dead_long]

duz_lat = [float(x) for x in duz_lat]
duz_long = [float(x) for x in duz_long]

farklar = []
for i in range(0,len(duz_lat)):
    duz_konum = (duz_lat[i], duz_long[i])
    dead_konum = (dead_lat[i], dead_long[i])
    farklar.append(geodesic(duz_konum, dead_konum).m)

print "Maximum aralik metre cinsinden: " + str(max(farklar))
indexler = farklar.index(max(farklar))
print "index of max element is " + str(indexler)
print duz_lat[indexler], " ", duz_long[indexler], " ", dead_lat[indexler], " ", dead_long[indexler]
dead = mpatches.Patch(color='red', label='Dead Reckoning')
gps = mpatches.Patch(color='blue', label='GPS')
plt.legend(handles=[dead,gps])
plt.scatter(dead_long,dead_lat, color='red')
plt.scatter(duz_long,duz_lat, color='blue')
#plt.plot((149.1692022, -35.3603534), (149.169274018, -35.3602605798))
plt.title("Dead Reckoning and GPS")
plt.show()
```

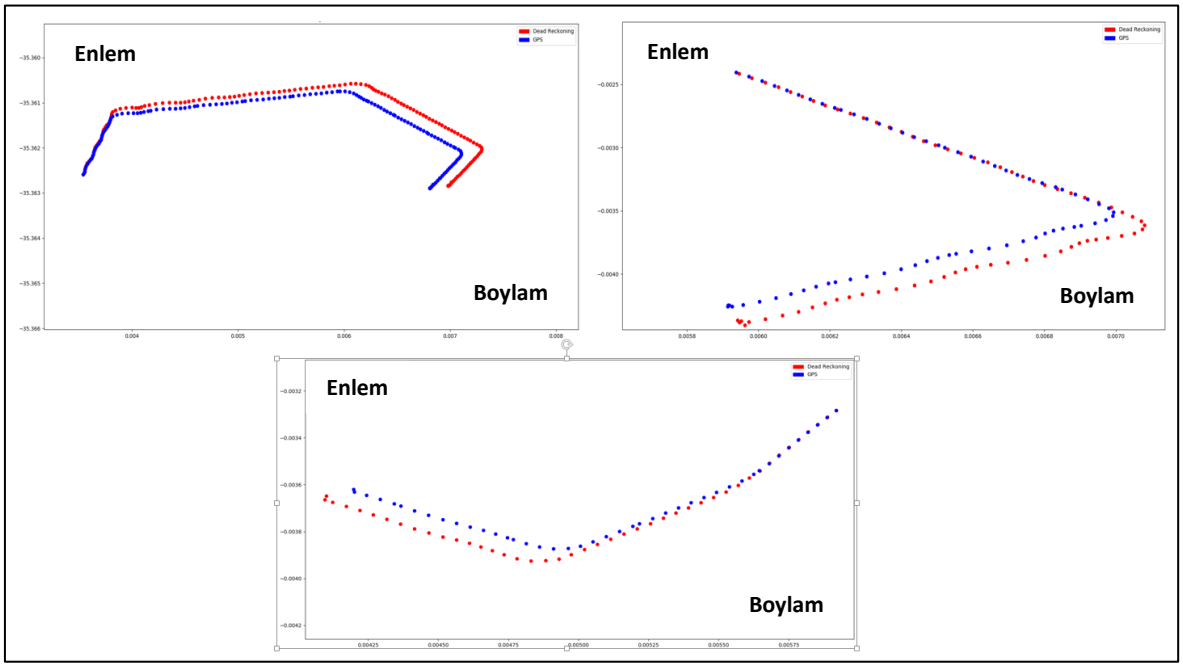
Şekil 6.19. Vincenty formülü – tahmin edilen konum verileri

Betikte görüldüğü gibi elde edilen tahmini konum verileri, GPS'ten elde edilen veriler ile aynı grafikte çizdirilmiştir. Şekil 6.20'de iki konum verileri de sunulmaktadır.



Şekil 6.20. GPS ve Dead Reckoning verileri

Aradaki farkın daha net izlenebilmesi için Şekil-6.21'de gösterilen 4 farklı uçuş planı daha oluşturularak gerekli hesaplamalar yapılmıştır.



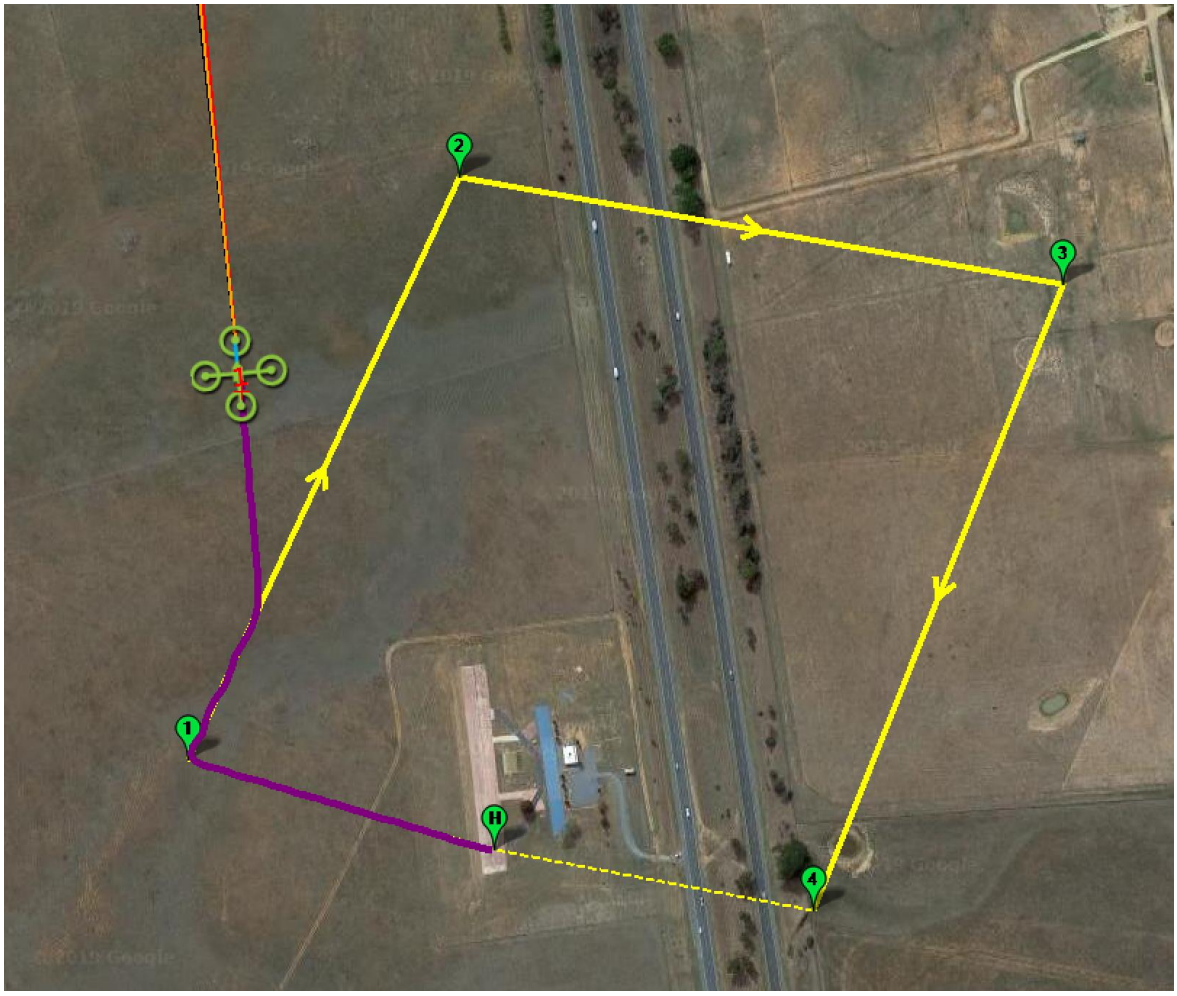
Şekil 6.21. Diğer uçuş planı verileri

5 ayrı test sonucunda maksimum konum farkları hesaplanmıştır. Keskin dönüşlere sahip uçuş planlarında konum farklarının daha fazla olduğu gözlemlenmiştir. Gerçekleştirilen testlerin ortalaması yaklaşık 18 metre olarak tespit edilmiştir.

Çizelge 6.2. Maksimum konum farkı

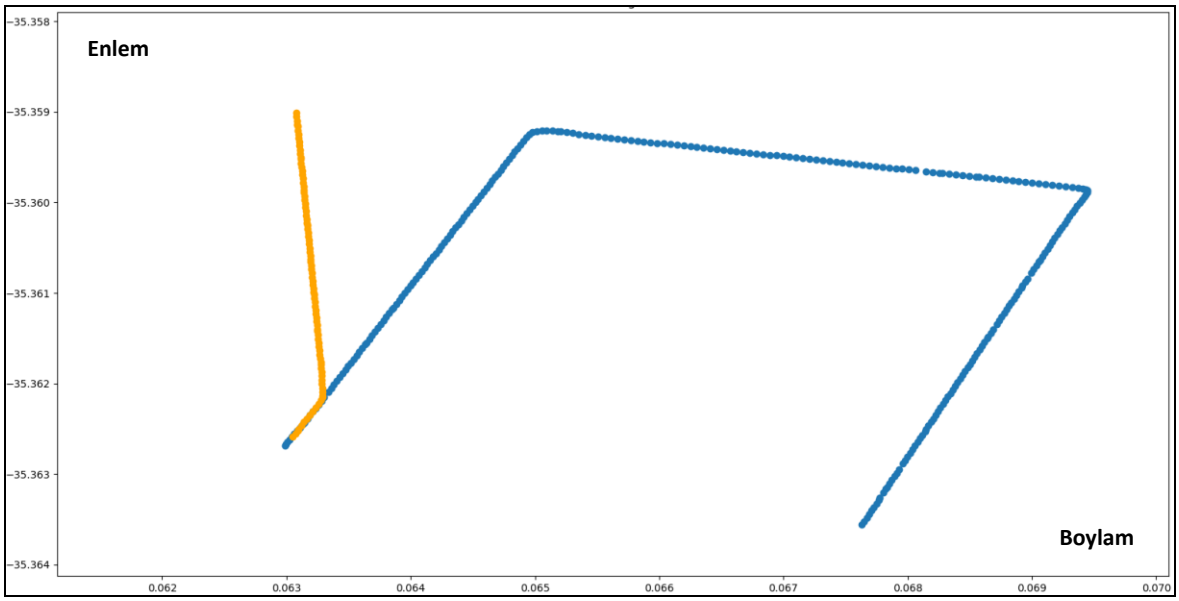
Test Sırası	Maksimum konum farkı (metre)	RMSE (metre)
1	12.19249	7.54835
2	24.24924	17.34235
3	15.37817	9.46149
4	27.36998	14.18401
5	10.50657	5.63056
Ortalama= 17.93929		

Mission Planner uygulaması üzerinde GPS aldatmacası senaryosu oluşturmak için uygulamanın dinamik olarak betik çalıştırma özelliğinden yararlanılmıştır. İHA, belirli bir uçuş rotasında uçarken GPS alıcısına farklı GPS verileri yüklenmiştir. Bu durumda İHA'nın Şekil 6.22'de görüldüğü gibi farklı bir yöne gittiği gözlemlenmiştir.



Şekil 6.22. GPS aldatmacası uygulanmış İHA

GPS aldatmacası uygulanan senaryoda sahte GPS koordinatları iletildikten sonra İHA'nın konum farkı ortalama değerin üzerine çıkarak artmaktadır. Şekil 6.23'te aldatmacaya ait çizim sunulmaktadır.



Şekil 6.23. GPS aldatmacası konum verileri

Aldatmaca saldırısı meydana gelmeden önce gözlemlenen konum farkı ortalama 18 metre civarında seyrederken, GPS aldatmacası gerçekleştirildikten sonra 18 metrenin çok üzerine çıkmıştır. Bu çalışmada konum farkı ortalamasının 18 metrenin üzerine çıkması anomali olarak değerlendirilmiştir.

6.6. GPS Konum Verilerinin Diğer GNSS Verileri ile Karşılaştırılması

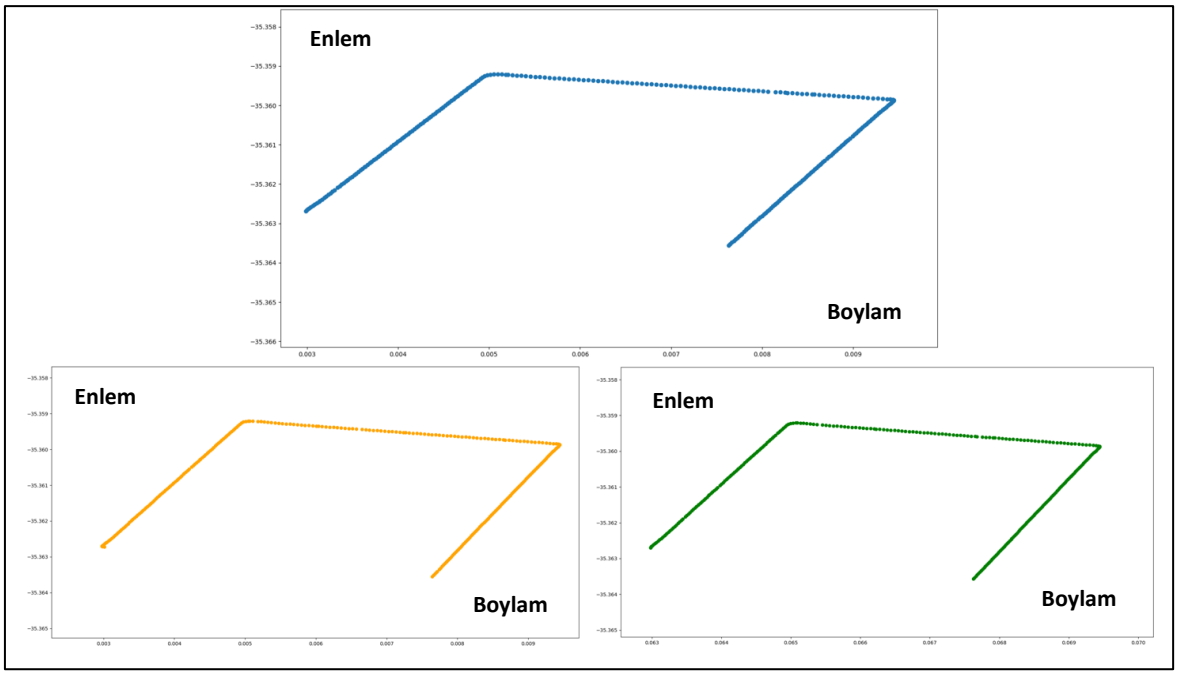
Teknolojinin hızlı gelişimi sayesinde gelişmiş donanımlar üretilmektedir. GPS alıcı modülleri de bu donanımlara örnek verilebilmektedir. Artık gelişmiş bir alıcı modülü GPS, GLONASS, BeiDou ve Galileo gibi konumlandırma sistemlerini aynı anda desteklemektedir. Böylece, GPS aldatmacası saldırılarının tespiti için karşılaştırma imkânı sağlanmaktadır.

Mission Planner uygulaması üzerinde de GPS_GNSS_MODE parametresi sayesinde belirtilen konumlandırma sistemlerinin test edilmesine imkân sunulmaktadır. Ön yüklü

olarak GPS ayarlı olarak gelmektedir. GLONASS için 64, BeiDou için 8 değerleri girilmektedir. Şekil 6.24'te konfigürasyon parametreleri sunulmaktadır.

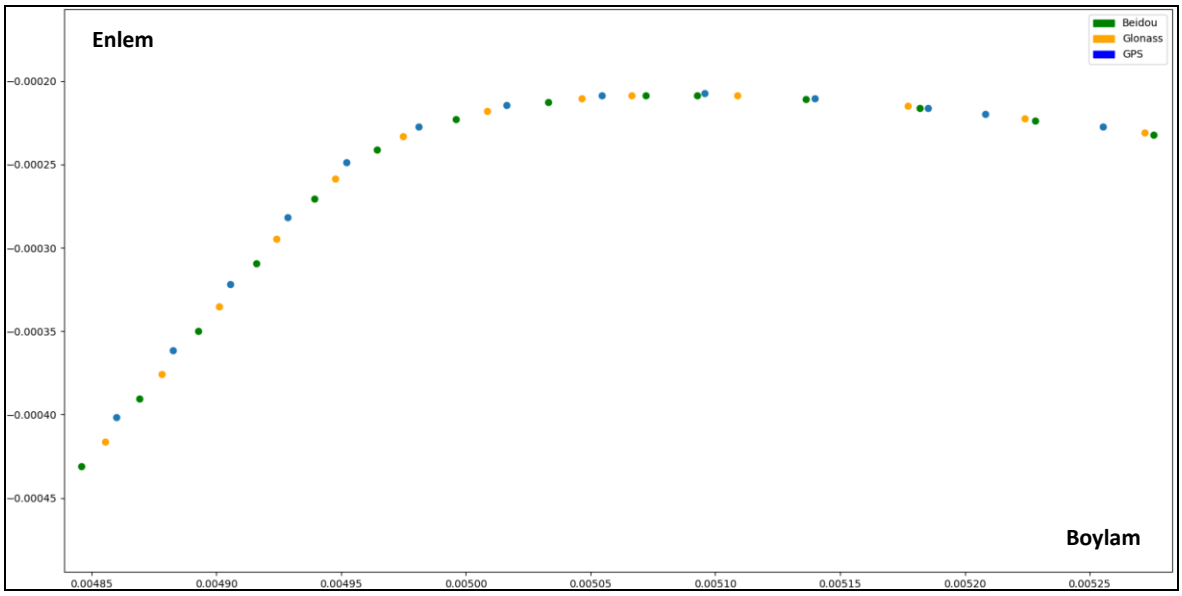
Şekil 6.24. Mission Planner GNSS konfigürasyon parametresi

Belirlenen bir rotaya göre Şekil 6.25'te GPS (mavi), Glonass (turuncu) ve BeiDou (yeşil) konum verilerine ait çizimler sunulmaktadır.



Şekil 6.25. GNSS konum verileri

Ayrıca, Şekil 6.26'da üç küresel konumlandırma sistemine ait veriler tek grafik üzerinde sunulmuştur. Elde edilen veriler doğrultusunda GPS-Glonass, GPS-BeiDou ve Glonass-BeiDou konum farkları metre cinsinden hesaplanmıştır.



Şekil 6.26. GPS, Glonass ve BeiDou konum verileri

GPS ve Glonass arasındaki konum farkı tutarlı değerlerde iken, GPS ve BeiDou konum farkı yaklaşık 500 metreye kadar ulaşabilmektedir. GPS aldatmacası tespitinde diğer GNSS sistemleriyle karşılaştırma yapılması durumunda Glonass'ın daha optimum bir çözüm olacağı değerlendirilmektedir.

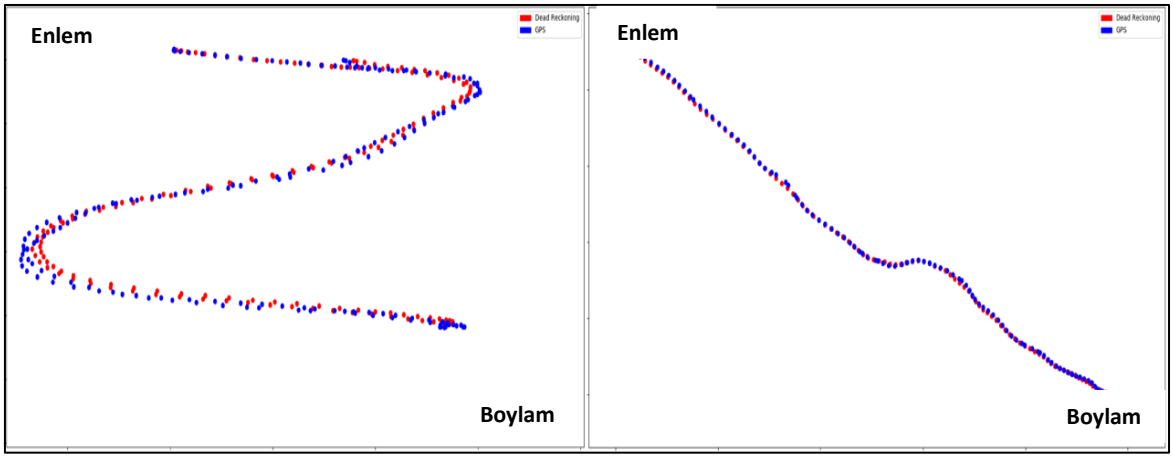
Yukarıda belirtilen GPS ve Glonass arasındaki 274 noktada hesaplanan konum farklarının ortalaması 14.49 metre olarak hesaplanmıştır. Maksimum konum farkının ise 23.08 metre olduğu gözlemlenmiştir. Bu değerin üstü anomali olarak değerlendirilmiştir.

6.7. Donanım Ortamında Gerçekleştirilen Test Çalışmaları

Donanım ile gerçekleştirilen test çalışmaları sırasında olası bir kazaya sebebiyet vermemek için yerleşim yerlerine uzak ve taşıt trafiğine kapalı bir alan tercih edilmiştir. Şekil 6.27'de testlerin gerçekleştirildiği ortam sunulmaktadır.

Şekil 6.27. Donanım test ortamı

Mission Planner uygulamasında daha önce test edilen uçuş senaryoları uygulanmadan 2 adet örnek uçuş güzergâhı oluşturularak test çalışmaları başlatılmıştır. Şekil 6.28'de belirtilen örnek senaryolara ait GPS verileri ve Vincenty işlemleri ile hesaplanan tahmini konum verileri sunulmaktadır.



Şekil 6.28. Örnek test senaryoları

Her iki örnek test uçuşu sırasında da GPS ve tahmini konum verileri farkının maksimum 18 metre civarında olduğu gözlemlenmiştir. Elde edilen veriler, Mission Planner uygulamasında gerçekleştirilen simülasyon ortamındaki test sonuçlarına çok yaklaşmıştır.

Daha sonra Mission Planner'ın üzerinde gerçekleştirilen simülasyon uçuş rotaları mevcut konum verisi üzerine yazdırılarak 5 adet senaryo gerçek zamanlı olarak test edilmiştir. Test sonucunda ulaşılan maksimum konum farklarına Çizelge 6.3'te yer verilmiştir.

Çizelge 6.3. Donanım testinden elde edilen maksimum konum farkı

Test Sırası	Maksimum konum farkı (metre)	RMSE (metre)
1	27.74992	15.28188
2	18.61970	10.54950
3	18.06145	10.25274
4	22.44271	14.18401
5	12.84935	4.90166
Ortalama= 19.94462		

Ortalama 20 metre konum farkı ile konum tahmini yapılarak test tamamlanmıştır. Ayrıca, diğer küresel konumlandırma sistemleri ile gerçekleştirilen testler neticesinde, GPS ve Glonass arasındaki maksimum konum farkının 33.17 metreye kadar ulaştığı gözlemlenmiştir. Analiz çalışmalarında testlerin gerçekleştirildiği ortam, hava durumu, kullanılan donanımların duyarlığı gibi etkenler de test sonuçlarını etkilemiştir.

Mission Planner uygulamasındaki simülasyon ortamı ve gerçek zamanlı test ortamı kullanılarak elde edilen verilerin yakın çıkması dikkat çekici bulunmuştur. Çalışma sonucunda, küresel konumlandırma sistemlerini hedef alan aldatmaca saldırının tespit edilmesi ve önlemesine yönelik Vincenty işlemleri ile konum tahmini yapılarak ve Glonass, BeiDou ve Galileo gibi konumlandırma sistemlerinden yararlanılarak başarılı sonuçlar elde edilmiştir. Özellikle, İHA sistemlerinde GPS sinyalinin aldatılması veya kesilmesi durumlarında belirtilen yöntemler kullanılarak yaşanabilecek kayıpların önüne geçilebilecektir.

7. SONUÇ VE ÖNERİLER

Son zamanlarda İHA'lar hayatımızın birçok alanında popüler bir şekilde kullanılmakta ve hızlı bir şekilde yaygınlaşmaktadır. Hassas konum ve otonom uçuş gibi özellikler sağlaması sebebiyle GNSS teknolojileri bu araçlar için vazgeçilmez bir bileşen haline gelmiştir. GPS, GLONASS, Galileo ve IRNSS gibi farklı ülkelere ait çeşitli GNSS sistemleri bulunmaktadır. Bu sistemler içinde en fazla olgunluk seviyesine GPS sistemi ulaşmıştır. Bunun doğal bir sonucu olarak son yıllarda sivil GPS kullanımı artmıştır.

Sivil GPS sinyali, yapısının açık, şifresiz ve herhangi bir kimlik doğrulama mekanizmasına sahip olmamasından dolayı aldatmaca saldırılarına karşı zafiyet barındırmaktadır. Bu çalışmada, insansız hava araçları tarafından kullanılan GPS sistemlerine yönelik gerçekleştirilen aldatmaca saldırıları ve bu saldırıları tespit etme yöntemleri incelenmiştir.

Literatürde yer alan GPS aldatmacası saldırıları ve tespit yöntemleri taranmıştır. Bu çalışmalar sinyal işleme, veri biti, pozisyon ve navigasyon çözümü seviyesi olmak üzere üç katmanda gerçekleştirilmektedir. İHA üzerindeki mevcut donanımlarla gerçekleştirilmesi ve yer istasyonu üzerinden hızlı bir şekilde analiz kolaylığı sağlamasından dolayı pozisyon ve navigasyon çözümü katmanı çalışmalarına odaklanılmıştır. AÖB sensör verileri ve diğer GNSS verileri üzerinden alınan konum verilerinin karşılaştırmalı analizinden etkili bir hibrit GPS aldatmacası tespit sistemi üzerinde çalışılmıştır. Ayrıca, bu tezle ile araştırmacılar için etkili bir kaynak sunulmuştur.

Analiz çalışmalarında literatürdeki GPS aldatmacası tespiti çalışmalarından farklı olarak Vincenty işlemleri kullanılmıştır. Çalışmalar neticesinde, hem simülasyon ortamında hem de donanım ortamında gerçek zamanlı olarak tasarlanan GPS aldatmacası senaryolarında başarılı bir şekilde aldatmaca tespiti gerçekleştirilmiştir. Ayrıca, kullanılan yöntemler, GPS gibi küresel konumlandırma sistemlerine erişim olmadığı durumlarda İHA'lara otonom uçuş kabiliyeti kazandırabilmektedir. Ancak Vincenty işlemlerinin daha net sonuç vermesi için kapsamlı GPS aldatmacası senaryosu verilerine ihtiyaç duyulmaktadır. İlerleyen çalışmalarda GPS aldatmacası veri seti oluşturulması ve GPS aldatmacası saldırısı sonucunda hava araçlarının tam kontrolünün sağlanması konusunda araştırmalar yapılması planlanmaktadır.

GPS aldatmacası saldırıları ile İHA'lar düşürülerek veya ele geçirilerek maddi kayıplara sebep olunabilmektedir. Yakın gelecekte GPS aldatmacası saldırı çeşitliliğinin ve tespit yöntemlerinin artacağı tahmin edilmektedir. Yapay zekâ, makine öğrenmesi, 5G ve nesnelerin interneti teknolojilerinin gelişmesiyle birlikte bu alanda çalışma yapacak araştırmacılar için yeni çalışma alanları sunulmaktadır. Küresel konumlandırma sistemlerindeki yenilikçi teknolojilerin yakından takip edilerek çalışmaların daha da artması ve ülkemizde yerli ve milli küresel konumlandırma sistemi çalışmalarına ağırlık verilmesi gerekmektedir.

KAYNAKLAR

1. Hell, P., Mezei, M. and Varga, P. J. (2017). Drone communications analysis, In *2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 213-216.

2. İnternet: Gps.gov, Official U.S. Government Information About The Global Positioning System (GPS) and Related Topics URL: http://www.gps.gov/, Son Erişim Tarihi: 06.02.2019.

3. Günther, C. (2014). A Survey of Spoofing and Counter-Measures. *Journal of the Institute of Navigation*, 61(3), 159-177.

4. Bernal, S. A. S. (2016). *Detection solution analysis for simplistic spoofing attacks in commercial mini and micro UAVs*. (MS thesis, University Of Tartu).

5. Qiao, Y., Zhang, Y. and Du, X. (2017). A Vision-Based GPS-Spoofing Detection Method for Small UAVs. In *2017 13th International Conference on Computational Intelligence and Security (CIS)*, IEEE, 312-316.

6. Su, J., He, J., Cheng, P. and Chen, J. (2016). A stealthy gps spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle. *IFAC-PapersOnLine*, 49(22), 291-296.

7. Huang, J., Presti, L. L., Motella, B. and Pini, M. (2016). GNSS spoofing detection: theoretical analysis and performance of the Ratio Test metric in open sky. *Ict Express*, 2(1), 37-40.

8. Wesson, K. D., Gross, J. N., Humphreys, T. E. and Evans, B. L. (2017). GNSS signal authentication via power and distortion monitoring. *IEEE Transactions on Aerospace and Electronic Systems*, 54(2), 739-754.

9. He, L., Li, W., Guo, C. and Niu, R. (2014). Civilian unmanned aerial vehicle vulnerability to gps spoofing attacks. In *2014 Seventh International Symposium on Computational Intelligence and Design*, IEEE, 2, 212-215.

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

11. Khalajmehrabadi, A., Gatsis, N., Akopian, D. and Taha, A. F. (2018). Real-time rejection and mitigation of time synchronization attacks on the global positioning system. *IEEE Transactions on Industrial Electronics*, 65(8), 6425-6435.

12. Panice, G., Luongo, S., Gigante, G., Pascarella, D., Benedetto, C. D., Vozella, A. and Pescape, A. (2017). A SVM-Based Detection Approach for GPS Spoofing Attacks to UAV. In *2017 23rd International Conference on Automation ve Computing (ICAC)*, IEEE, 1-11.

13. O'Hanlon, B. W., Psiaki, M. L., Bhatti, J. A., Shepard, D. P. and Humphreys, T. E. (2013). Real-Time GPS Spoofing Detection Via Correlation of Encrypted Signals. *Navigation*, 60(4), 267-278.

14. Psiaki, M. L., Humphreys, T. E. (2016). GNSS Spoofing and Detection. *Proceedings of the IEEE*, 104(6), 1258-1270.

15. İnternet: Amazon Resmi Sayfası Amazon Prime Air URL: https://www.amazon.com/, Son Erişim Tarihi: 06.02.2019.

16. Doğru, İ. A., Dörterler, M. & Uyar E. (2019). *İnsansız Hava Araçları ve Siber Güvenlik.* Siber Güvenlik ve Savunma: Problemler ve Çözümler (Sağıroğlu Ş. & Şenol M., Ed.). Ankara: Grafiker Yayınları, 15, 517-534.

17. Rodday, N. M. (2015). *Exploring Security Vulnerabilities of Unmanned Aerial Vehicles*. (MS thesis, University of Twente).

18. Rodday, N. (2016). Hacking a Professional Drone, *RSA Conference*, San Francisco.

19. Javaid, A. Y. (2015). *Cyber security threat analysis and attack simulation for unmanned aerial vehicle network*. (Doctoral dissertation, University of Toledo).

20. He, D., Chan, S. and Guizani, M. (2017). Drone-Assisted Public Safety Networks: The Security Aspect. *IEEE Communications Magazine*, 55(8), 218-223.

21. Javaid, A. Y., Alam, M., Sun, W. and Devabhaktuni, V. K. (2012). Cyber Security Threat Analysis and Modelling of an Unmanned Aerial Vehicle System. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 585-590.

22. Haider, Z., Khalid, S. (2016). Survey on Effective GPS Spoofing Countermeasures. In *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, 573-577.

23. İnternet: Atis Standart: GPS Vulnerability URL: https://access.atis.org/apps/group_public/download.php/36304/ATIS-0900005.pdf, Son Erişim Tarihi: 08.06.2019.

24. İnternet: ArduPilot Geliştirici Sayfası URL: http://ardupilot.org/copter/docs/common-apm25-and-26-overview.html, Son Erişim Tarihi: 01.06.2019.

25. İnternet: U-BLOX Bilgilendirme Sayfası URL: https://www.u-blox.com/sites/default/files/NEO-M8-FW3_DataSheet_%28UBX-15031086%29.pdf, Son Erişim Tarihi: 10.06.2019.

26. İnternet: ArduPilot Mission Planner İnceleme Sayfası URL: http://ardupilot.org/planner/docs/mission-planner-overview.html, Son Erişim Tarihi: 08.06.2019.

27. İnternet: MAVLink Protokolü Geliştirici Sayfası URL: https://mavlink.io/, Son Erişim Tarihi: 27.05.2019.

28. İnternet: MAVLink Protokolü Github Geliştirici Sayfası URL: https://github.com/mavlink/mavlink-devguide/, Son Erişim Tarihi: 27.05.2019.

29. Kwon, Y. M., Yu, J., Cho, B. M., Eun, Y. and Park, K. J. (2018). Empirical Analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles. *IEEE Access*, 6, 43203-43212.

30. Vincenty, T. (1975). Direct And Inverse Solutions Of Geodesics On The Ellipsoid With Application of Nested Equations. *Survey Review*, 23(176), 88-93.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: UYAR, Emre
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 27.10.1990, Ankara
Medeni hali	: Bekar
e-mail	: emre.uyar@gazi.edu.tr

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Yüksek lisans	Gazi Üniversitesi / Bilgi Güvenliği Mühendisliği	Devam Ediyor
Lisans	Eskişehir Osmangazi Üniversitesi / Elektrik-Elektronik Mühendisliği	2014
Lise	Kızılcahamam Anadolu Lisesi	2008

İş Deneyimi

Yıl	**Yer**	**Görev**
2014 - Halen	İnnova Bilişim Çözümleri A.Ş.	Bilgi Teknolojileri Uzmanı

Yabancı Dil

İngilizce

Yayınlar

1. Uyar, E., Dogru, İ.A., Dorterler, M. (2019). The Detection Methods of GPS Spoofing on Unmanned Aerial Vehicles, *Turkish Journal of Mathematics and Computer Science* (Accepted). (Kabul edildi)

Hobiler

Müzik, Futbol, Puzzle

GAZİ GELECEKTİR...