TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ALDATMA SALDIRISI TESPİTİ VE ALDATMAYA KARŞI ÖNLEM İÇİN KALMAN FİLTRESİ TASARIMI

YÜKSEK LİSANS TEZİ

Hande Işıl AKÇAY

Elektrik ve Elektronik Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof. Dr. Tolga GİRİCİ

MAYIS 2023

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

Hande Işıl AKÇAY

İMZA

ÖZET

Yüksek Lisans Tezi

ALDATMA SALDIRISI TESPİTİ VE ALDATMAYA KARŞI ÖNLEM İÇİN KALMAN FİLTRESİ TASARIMI

Hande Işıl AKÇAY

TOBB Ekonomi ve Teknoloji Üniversitesi
Fen Bilimleri Enstitüsü
Elektrik ve Elektronik Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Tolga GİRİCİ

Eş Danışman: Dr. Emrah ONAT

Tarih: Mayıs 2023

Küresel konumlama sistemleri (KKS) ölçümlerinin konumlama çözümlerinde kullanılmasının yaygınlaşması ve özellikle otonom araç navigasyonunun temelini oluşturmasıyla, bu sistemlerden alınan ölçüm doğruluklarının önemi artmıştır. Öte yandan, aldatma saldırıları ile KKS alıcılarının gerçekten farklı konumlama çözümü elde edip aldanmasının sağlanması üzerine uygulamalar da son yıllarda yaygınlaşmaya başlamıştır. Dolayısıyla, KKS alıcıları içerisinde, olası aldatma saldırılarına karşı tespit ve karşı tedbir algoritmalarının eklenmesi oldukça kritik önem taşımaktadır. Aldatma tespit ve aldatmaya karşı önlem için KKS alıcıları içerisinde geliştirilen pek çok farklı yöntem bulunmakta olup, bu yöntemler alıcı yapısının farklı kısımlarına kullanılmak üzere önerilmektedir. Bu çalışma kapsamında, günümüzde aktif olarak küresel konumlama hizmeti sunan GPS, Galileo, GLONASS, BeiDou sistemleri ile konumlama çözümü üreten, hareketli bir araç üzerindeki KKS alıcısı içerisinde, aldatma tespiti ve aldatmaya karşı tedbir amacıyla kullanılmak üzere Kalman filtresi tasarımı sunulmaktadır. Önerilen bu filtre, KKS alıcısının farklı konumlama sistemlerinden aldığı sinyaller ile konumlama çözümü ürettikten sonra, nihai pozisyon çözümünü sunmadan hemen önceki navigasyon bloğunda kullanılmak üzere tasarlanmıştır. Çalışmaların ilk bölümünde tasarlanan algoritma, farklı KKS ölçümleri

artıklık hesaplarının karşılaştırılması yöntemini esas alarak aldatma tespiti yapmakta, ardından aldatma olmayan sistem ölçümlerini kullanarak konumlama çözümü üretmeye devam etmektedir. Bu algoritmaya ek olarak, çalışmaların ikinci bölümünde, KKS alıcısının içerisine entegre edilecek bir ivmeölçer ile konumlama çözümleri üretilmesi modellenmiştir. Bu çözümlerle artıklık hesaplarının da KKS artıklıkları ile karşılaştırılması algoritmaya dahil edilmiştir. İvmeölçerin de sisteme entegre edilmesi ile olası aldatma senaryolarının sayısının arttırılması sağlanmıştır. Tasarlanan filtrenin başarımı Monte-Carlo simülasyonları ile test edilmiştir. Farklı aldatma yörüngeleri oluşturularak, bu yörüngelerde aldatma saldırılarının uygulanabileceği olası tüm senaryolar altında filtrenin performansı yüzde tespit başarımı ve tespit süresi cinsinden incelenmiştir. Oluşturulan aldatma yörüngeleri için, uygulanan aldatma senaryolarındaki baskın ve resesif olan KKS'lerin pozisyon doğrulukları ile tespit süreleri arasındaki ilişki açıklanmıştır. Son olarak, filtrenin aldatma tespiti yapmak için kullandığı eşik değerinin farklı seviyeler için test edilmesi ile alıcı çalışma karakteristiği eğrileri çizdirilmiş, bu eğrilerin altında kalan alanların hesaplanması ile filtrenin farklı aldatma yörüngelerindeki başarımları verilmiştir.

Anahtar Kelimeler: Küresel konumlama sistemleri, Kalman filtresi, Aldatma tespiti, Alıcı çalışma karakteristiği.

ABSTRACT

Master of Science

KALMAN FILTER DESIGN FOR SPOOFING ATTACK DETECTION AND ANTI-SPOOFING

Hande Işıl AKÇAY

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Electrical and Electronics Engineering Science Programme

Advisor: Prof. Dr. Tolga GİRİCİ

Co-Advisor: Dr. Emrah ONAT

Date: May 2023

With the widespread use of global navigation satellite systems (GNSS) measurements in positioning solutions and especially forming the basis of autonomous vehicle navigation, the importance of measurement accuracy from these systems has increased. On the other hand, applications have also started to become widespread in recent years, for spoofing attacks, ensuring that the GNSS receivers obtain incorrect positioning solutions. Therefore, adding detection and countermeasure algorithms, within GNSS receivers, against possible spoofing attacks is critically important. For spoofing detection and countermeasure, there are many different methods developed within GNSS receivers, and these methods are recommended for use in different parts of the receiver structure. Within the scope of this study, in order to detect and prevent the spoofing attack a Kalman filter design is presented for use in a GNSS receiver mounted on an autonomous moving vehicle, which provides a positioning solution by using GPS, Galileo, GLONASS, and BeiDou systems, that are actively providing global positioning services. This proposed filter is designed to be used in the navigation block, just before presenting the final position solution, after generating a positioning solution with the signals received by the GNSS receiver from different positioning systems. The algorithm designed in the first part of the studies detects

spoofing, based on the method of comparing the residual calculations of different GNSS measurements, and then continues to produce a positioning solution using non-spoofed system measurements. In addition to this algorithm, in the second part of the studies, generating positioning solutions with an accelerometer to be integrated into the GNSS receiver is modeled. The comparison of the residuals calculated by using these solutions with the GNSS residuals is included in the algorithm. By integrating the accelerometer into the system, the number of possible spoofing scenarios is increased. The performance of the designed filter has been tested with Monte-Carlo simulations. By creating different spoofing trajectories, the performance of the filter is examined in terms of percentage spoofing detection performance and detection time under all possible scenarios in which spoofing attacks can be applied in these trajectories. For the created spoofing trajectories, the relationship between the dominant and recessive GNSS position accuracies and detection times is explained in the applied spoofing scenarios. Finally, by testing the threshold value used by the filter to detect spoofing for different levels, receiver operating characteristics curves were drawn, and the performances of the filter in different spoofing trajectories were given by calculating the areas under these curves.

Keywords: Global navigation satellite systems, Kalman filter, Spoofing detection, Receiver operating characteristics.

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren hocam Prof. Dr. Tolga GİRİCİ'ye ve Dr. Emrah ONAT'a, araştırma bursundan faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi'ne, beni bu yeni konu ile tanıştıran şirketim Meteksan Savunma'ya, bu çalışma sürecinde bana destek olan Mehmet Buğrahan ÜSTÜNDAĞ'a, destekleriyle her zaman yanımda olan Ahmet Emre AÇIKGÖZ'e, aileme ve arkadaşlarıma çok teşekkür ederim.

İÇİNDEKİLER

Sayfa

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

KISALTMALAR

ADC : Analog-Dijital Dönüştürücü (Analog-to-Digital Converter)
AGC : Otomatik Kazanç Kontrolü (Automatic Gain Control)
ANS : Ataletsel Navigasyon Sistemi (Inertial Navigation System, INS)
AÖB : Ataletsel Ölçüm Birimi (Inertial Measurement Unit, IMU)
DLL : Gecikme Kilitli Döngü (Delay Locked Loop)
DOP : Hassasiyet Seyreltilmesi (Dilution of Precision)
ECEF : Yer Merkezli-Yer Sabit (Earth-Centered Earth-Fixed)
EKF : Genişletilmiş Kalman Filtresi (Extended Kalman Filter)
GDOP : Geometrik Hassasiyet Seyreltilmesi (Geometric Dilution of Precision)
GEO : Jeostatik Yörünge (Geosynchronous Orbit)
GPS : Küresel Konumlandırma Sistemi (Global Positioning System)
HDOP : Yatay Hassasiyet Seyreltilmesi (Horizontal Dilution of Precision)
IF : Ara Frekans (Intermediate Frequency)
IGSO : Eğik Jeostatik Yörünge (Inclined Geosynchronous Orbit)
KF : Kalman Filtresi (Kalman Filter)
KKS : Küresel Konumlama Sistemi (Global Navigation Satellite System, GNSS)
LiDAR : Işık Tespiti ve Uzaklık Tayini (Light Detection and Ranging)
MEMS : Mikroelektro-Mekanik Sistemler (Microelectro-Mechanical Systems)
MEO : Orta Dünya Yörüngesi (Medium Earth Orbit)
NED : Kuzey-Doğu-Aşağı (North-East-Down)
PDOP : Pozisyon Hassasiyet Seyreltilmesi (Position Dilution of Precision)
PLL : Faz Kilitli Döngü (Phase Locked Loop)
PRN : Sözde Rastgele Gürültü (PseudoRandom Noise)
RAIM : Alıcı Otonom Bütünlük İzlenmesi (Receiver Autonomous Integrity Monitoring)
RF : Radyo Frekansı (Radio Frequency)
ROC : Alıcı Çalışma Karakteristiği (Receiver Operating Characteristic)
SDR : Yazılım Tanımlı Radyo (Software Defined Radio)
SQM : Sinyal Kalitesi İzlenmesi (Signal Quality Monitoring)
UERE : Kullanıcı Eşdeğer Aralık Hatası (User Equivalent Range Error)
UKF : Kokusuz Kalman Filtresi (Unscented Kalman Filter)

SEMBOL LİSTESİ

Bu çalışmada kullanılmış olan simgeler açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
c	Işık hızı
dt	Örnekleme zaman aralığı
ρ	Sözde menzil
D	Uydu ile alıcı arası gerçek menzil
Δt	Zaman gecikmesi
d	Sözde menzil hata bileşeni
$x_{uydu}, y_{uydu}, z_{uydu}$	Uydu konumları
$x_{alıcı}, y_{alıcı}, z_{alıcı}$	Alıcı konumları
N	Görünür uydu sayısı
σ	Pozisyon doğruluğu
$D_{N/E}$	NED'den ECEF'e dönüşüm matrisi
$D_{E/N}$	ECEF'ten NED'e dönüşüm matrisi
x_0	Başlangıç durumları
poz_x, poz_y, poz_z	Başlangıç pozisyonları
n	KKS numarası
x_k	k zaman anındaki durum vektörü
z_k	k zaman anındaki ölçüm vektörü
n_k	Sistem gürültü bileşeni
v_k	Ölçüm gürültü bileşeni
$\hat{x}_k, \hat{a}_k$	k zaman anındaki durum kestirimleri
$\hat{x}_k^-, \hat{a}_k^-$	k zaman anındaki durum tahminleri
P_k^-	k zaman anındaki hata kovaryansı tahminleri
$\hat{y}_k$	k zaman anındaki inovasyon
$r_{k,n}$	k zaman anındaki n'inci KKS için artıklık (residual) değeri
$r_{k,ANS}^x$	k zaman anındaki ölçüm güncellemesi yapıldığında ANS artıklık değeri
$r_{k,ANS}^a$	k zaman anındaki ölçüm güncellemesi yapılmadığında ANS artıklık değeri
K_k	k zaman anındaki Kalman kazancı
$\overline{K_k}$	k zaman anındaki ortalama Kalman kazancı
P	Hata kovaryans matrisi

F	Durum dönüşüm matrisi
Q	Durum hata kovaryans matrisi
R	Ölçüm hata kovaryans matrisi
I	Birim matris
0	Sıfır matrisi
H	Gözlem matrisi
$\tilde{a}_x, \tilde{a}_y, \tilde{a}_z$	İvmeölçer ivme tahminleri
$\tilde{w}_x, \tilde{w}_y, \tilde{w}_z$	Dönüölçer dönü tahminleri
a_x, a_y, a_z	Gerçek ivme değerleri
w_x, w_y, w_z	Gerçek dönü değerleri
S_x, S_y, S_z	Orantı katsayısı hataları
B_x, B_y, B_z	Sabit kayma (bias) hataları
η_x, η_y, η_z	Stokastik hatalar
$M_{xy}, M_{xz}, M_{yx},$ M_{yz}, M_{zx}, M_{zy}	Eksen kaçıklığı hataları
Y	Aldatma yörüngesi katsayısı
x_{NED}, y_{NED}	NED koordinat sisteminde pozisyonlar

1. GİRİŞ

Küresel konumlama sistemleri (KKS / Global Navigation Satellite Systems (GNSS)), Dünya yörüngesinde dönen uydu takımlarından oluşmaktadır. Günümüzde GPS, Galileo, GLONASS ve BeiDou olmak üzere 4 farklı küresel konumlama sistemi mevcuttur. Bu sistemlerin uydularından iletilen sinyaller sayesinde, yeryüzündeki kullanıcılara gerçek zamanlı olarak üç-boyutlu konum, hız ve zaman bilgileri sağlanabilmektedir [1-4].

KKS uyduları ile alıcı arasındaki mesafe, alıcının anten kazancı, boşluk zayıflaması (free-space path loss) gibi etkenlerden dolayı alıcının aldığı sinyal gücü seviyesi oldukça düşüktür [5]. Dolayısıyla, karıştırma ve aldatma gibi elektronik saldırılara karşı oldukça hassaslardır [6].

Aldatma saldırılarının amacı; KKS alıcısının doğru olmayan konum ve/veya zaman tahmini yapmasını sağlamaktır [7].

Aldatma saldırıları; sinyal geciktirme (meaconing) ve sinyal sentezleme (spoofing) olmak üzere iki ana başlıkta incelenebilmektedir. Sinyal geciktirme yönteminde, gerçek KKS uydularından alınan sinyaller kaydedilmekte ve belli bir zaman sonra aldatıcı tarafından yeniden yayınlanmaktadır. Sinyal sentezleme yönteminde ise, hedef alıcının kendini başka bir konumda olduğunu zannetmesini sağlayacak şekilde uydu navigasyon mesajları yeniden üretilerek yayınlanmaktadır [6,8].

Aldatma saldırısı uygulanacak herhangi bir hedef alıcının, kendi yörüngesinden saparak hedeflenen aldatma yörüngesine yönelmesini sağlayabilmek için, yazılım tanımlı radyo (SDR, software defined radio) veya KKS sinyal simülatörleri yardımıyla üretilen aldatma yörüngesi noktalarına göre aldatma sinyalleri üretilebilmektedir. Hedef alıcının bu aldatma yörüngesini takip ederek yanıltılması amaçlanmaktadır [6].

Özellikle elektronik harp alanında, son yıllarda elektronik aldatma saldırıları uygulamalarının yaygınlaşması sebebiyle, bu saldırıların KKS alıcıları tarafından tespit edilebilmesi ve karşı tedbirlerinin alınabilmesi oldukça önem kazanmıştır [9].

Bu tezin ilk bölümünde, konu hakkında genel bilgiler verilerek tezin amacı belirlenmekte ve bu kapsamda literatür araştırmaları sunulmaktadır. Tezin ikinci

bölümünde, GPS, Galileo, GLONASS, BeiDou sistemleri ile konumlama çözümü üreten bir KKS alıcısı için tasarlanan Kalman filtresi yaklaşımı önerilmektedir. Üçüncü bölümde, bu sisteme ivmeölçer eklenmesi ile geliştirilen filtre tasarımı sunulmaktadır. Tezin son bölümünde ise elde edilen sonuçlar özetlenmekte ve öneriler yer almaktadır.

1.1 Tezin Amacı

Küresel konumlama sistemlerine karşı aldatma saldırılarının yapılarak alıcıların kendilerini farklı bir konumda olduklarını zannetmelerinin sağlanması, ya da takip etmekte olduğu hareket yörüngesinden saparak üretilen aldatma yörüngesine girmesinin sağlanması, özellikle elektronik harp alanında son yıllarda yaygın olarak kullanılmaya başlanmıştır. Dolayısıyla, hedef alıcılarda bu saldırıların tespit edilerek karşı tedbirlerin geliştirilebilmesi son derece kritik önem taşımaktadır [9].

Bu tez çalışması kapsamında; aldatma saldırılarına karşı, KKS alıcısı içerisinde tasarlanacak bir Kalman filtresi yaklaşımı ile aldatma saldırısı tespiti ve saldırıya karşı önlem alınabilmesi sağlanması amaçlanmaktadır.

Yapılan çalışmaların ilk bölümü; günümüzde mevcut olan 4 farklı KKS'yi kullanan bir alıcının, bu sistemlerden gelen pozisyon çözümlerinin Kalman filtresi yardımıyla karşılaştırılarak, olası aldatma saldırısı tespiti ve karşı önlemin alınabilmesi üzerinedir. Çalışmaların ikinci bölümünde ise; KKS alıcısına entegre edilmiş bir ivmeölçer ile, çoklu KKS aldatma senaryoları altında da çalışabilen bir filtre tasarımı sunulması amaçlanmaktadır.

KKS alıcısının nihai konumlama çözümünü üretmeden hemen önceki navigasyon bloğunda kullanılması üzerine önerilen bu Kalman filtresi yaklaşımı ile, alıcıların aldatma saldırılarına karşı önlemlerinin arttırılmış olması amaçlanmıştır. KKS alıcısının diğer bloklarında olası aldatma saldırılarına karşı çeşitli tedbirler alınmış olmasına rağmen tespitinin yapılamamış olması ihtimaline karşı, alıcının son bloğunda da geliştirilen algoritma ile aldatma tespit ve karşı önlem performansının arttırılması hedeflenmektedir.

1.2 Literatür Araştırması

1.2.1 Küresel konumlama sistemleri hakkında genel bilgiler

Günümüzde GPS, Galileo, GLONASS, BeiDou olmak üzere 4 farklı küresel konumlama sistemi (KKS) mevcuttur. Küresel konumlama sistemleri; birbirini tamamlayan üç temel segmentten oluşmaktadır. Bunlardan ilki uzay segmentidir. Dünya etrafında planlanmış belirli yörüngelerde dönen ve dönerken yeryüzüne konumlama sinyali gönderen uydular uzay segmentini oluşturmaktadır. Sistemin ikinci temel bileşeni kontrol segmentidir. Kontrol segmenti; yeryüzüne yerleştirilmiş izleme istasyonları, yer kontrol istasyonları ve antenlerden oluşmaktadır. Sistemin üçüncü temel bileşeni ise kullanıcı segmentidir. Kullanıcı segmenti, uydulardan yayınlanan konumlama sinyallerini yakalayan ve bu sinyalleri işleyerek konum bilgisi üreten elektronik kullanıcı ekipmanları ile kullanıcılarını kapsamaktadır [2, 10].

GPS; tam adı NAVSTAR GPS (Navigation System with Timing and Ranging Global Positioning System) olup, ilk uydusunu 1978 yılında fırlatarak ilk küresel konumlama sistemi olmuştur. Amerika Birleşik Devletleri'ne ait bu sistem, günümüzde 31'i operasyonel toplam 32 uydudan oluşmakta olup, uyduları yeryüzünden yaklaşık 20,200 km uzaklıktaki yörüngelerde hareket etmektedir [2, 11].

Galileo, 1990'lı yılların başlarında Avrupa Birliği tarafından geliştirilmiş küresel konumlama sistemidir. 23,222 km uzaklıktaki dairesel yörüngelerinde toplam 30 uydusu bulunmaktadır [2, 12].

GLONASS, Rusya tarafından geliştirilmiş olup, yeryüzünden 19,100 km uzaklıktaki toplam 24 uydudan oluşmaktadır. Uydular, üç yörünge düzleminde ve her düzlemde 8 uydu olacak şekilde yerleştirilmiştir [2, 13].

BeiDou, Çin tarafından geliştirilen, 5 GEO (jeostatik yörünge, Geosynchronous Orbit), 3 IGSO (Eğik jeostatik yörünge, Inclined Geosynchronous Orbit) ve 27 MEO (Orta Dünya yörüngesi, Medium Earth Orbit) uyduları olmak üzere toplam 35 uydudan oluşan sistemdir. BeiDou sisteminin GEO ve IGSO uyduları 35,786 km uzaklıkta, MEO uyduları ise 21,528 km uzaklıktaki yörüngelerde olacak şekilde tasarlanmıştır [2, 14].

KKS sinyalleri, frekans spektrumunda alt ve üst L bantta, sırasıyla yaklaşık 1160-1300 MHz ve 1550-1610 MHz frekans aralıklarında yer almaktadır. KKS sistem uyduları tarafından belirli merkez frekansı, kodlama frekansı, modülasyon, bant genişlikleri gibi özellikler ile navigasyon sinyalleri yayınlanmakta ve yeryüzündeki alıcılara olabildiğince yüksek doğrulukta konumlama çözümü sunulması amaçlanmaktadır. Uydular tarafından yayınlanan efemeris ve almanak bilgileri temel olarak o uyduya ait konum ve zaman verilerini taşımaktadır [2].

1.2.2 KKS alıcısı ile konumlama hesabı

Alıcı tarafında konumlama çözümünün yapılabilmesi için, en az 4 farklı görünür uydudan alınan sinyaller sayesinde, uydularla alıcı arasındaki sözde menziller (pseudo range) ölçümlenmektedir. Sözde menzil (ρ) hesabı Eşitlik (1.1)'deki gibi ifade edilebilmekte olup, her uydu için ayrı ayrı hesaplanmakta, gerçek menzil ve çeşitli hata kaynaklarından oluşmaktadır [15].

$$\rho = D + c.\Delta t - d_{uydu} + d_{iyono} + d_{tropo} + d_{rel} + d_{araç} \qquad (1.1)$$

Burada, D uydu ile alıcı arasındaki gerçek mesafedir. c ışık hızı, Δt zaman gecikmesi olup; $c.\Delta t$ bileşeni, alıcı saatinin sistem zamanından kaymasının neden olduğu bilinmeyen mesafeyi yansıtmaktadır. d_{uydu} bileşeni KKS sistem zamanının uydu saatine göre ilerlemesinden kaynaklanan hata parametresidir. Sırasıyla d_{iyono} ve d_{tropo} bileşenleri, iyonosferik ve troposferik gecikmelerden kaynaklanmaktadır. d_{rel} ve $d_{araç}$ bileşenleri ise sırasıyla relativistik (göreceli) ve alıcıdan kaynaklanabilecek araçsal gecikme hatalarıdır.

d_{uydu}, d_{iyono}, d_{tropo}, d_{rel}, $d_{araç}$ bileşenleri genellikle çok düşük seviyelerde olduğundan ihmal edilerek Eşitlik (1.2)'deki gibi formülün sadeleştirilmesi sağlanabilmektedir.

$$\rho = D + c.\Delta t \tag{1.2}$$

D, alıcı ile uydu arasındaki geometrik mesafe olduğundan Eşitlik (1.3)'teki gibi ifade edilebilmektedir. Burada x_{uydu}, y_{uydu}, z_{uydu} ifadeleri uydunun, $x_{alıcı}$, $y_{alıcı}$, $z_{alıcı}$ ifadeleri ise alıcının x-y-z eksenlerindeki konum bilgileridir.

$$\rho = \sqrt{(x_{uydu} - x_{alıcı})^2 + (y_{uydu} - y_{alıcı})^2 + (z_{uydu} - z_{alıcı})^2} + c.\Delta t \tag{1.3}$$

Eşitlik (1.3)'teki $x_{alıcı}$, $y_{alıcı}$, $z_{alıcı}$ ve Δt ifadeleri bilinmeyenler olup, doğrusal olmayan bu denklem setinin çözülebilmesi için en az 4 farklı sözde menzil eşitliğine ihtiyaç duyulmaktadır. Bu sebeple, en az 4 adet olmak üzere N farklı uydudan alınan uydu konumları bilgisi ile, N adet sözde menzil denklem kümesi oluşturularak, doğrusallaştırmaya dayalı iteratif teknikler ile çözümlendirilmektedir [15].

Konumlama çözümünde kullanılan uydu sayısının arttırılması ile konumlama performansı artırılabilmektedir. Dolayısıyla, farklı konumlama sistemi uydularının da entegre olarak kullanılmasıyla daha yüksek hassasiyette pozisyon çözümleri elde edilebilmektedir.

Bir KKS alıcısında, konumlama çözümü yaparken kullanacağı uyduların optimal bir şekilde seçilebilmesi, olabildiğince az işlem yükü ile olabildiğince gerçeğe yakın pozisyonlama çözümleri sunulabilmesi açısından kritiktir. Daha iyi bir geometrik dağılıma sahip uydu kombinasyonu ile daha iyi konumlama doğruluklarına erişilebilmektedir. Geometrik hassasiyet seyreltilmesi (geometric dilution of precision, GDOP), uydu geometrisinin konumsal ölçüm hassasiyeti üzerindeki matematiksel bir etkisi olarak hata yayılımını belirtmek için kullanılan bir terimdir ve görünür uydular arasından kullanılacak uyduların seçiminde bir ölçüm olarak kullanılmaktadır. Küçük bir GDOP değeri büyük GDOP değerlerine göre, uydu geometrilerinin daha iyi olduğunu göstermektedir. Uyduların gökyüzündeki yerleşimleri ne kadar dağınıksa, GDOP değeri o kadar küçüktür. Aksine, uyduların dağılımı bir bölgeye ne kadar yoğunlaşırsa GDOP değeri o kadar büyük olur [16].

GDOP hesabı için, Eşitlik (1.4)'te verildiği gibi, N adet görülebilir uydu için N satır sayılı, üç-boyutlu konum ve zaman sapması bilinmeyenleri için 4 sütunlu bir G matrisi oluşturulmaktadır.

$$G = \begin{bmatrix} x_1 & y_1 & z_1 & -1 \\ \vdots & \vdots & \vdots & \vdots \\ x_N & y_N & z_N & -1 \end{bmatrix} \tag{1.4}$$

G matrisinden faydalanılarak, A matrisi Eşitlik (1.5)'te verildiği gibi tanımlanmaktadır.

$$A = [G^T G]^{-1} = \begin{bmatrix} a_{11}\ a_{12}\ a_{13}\ a_{14} \\ a_{21}\ a_{22}\ a_{23}\ a_{24} \\ a_{31}\ a_{32}\ a_{33}\ a_{34} \\ a_{41}\ a_{42}\ a_{43}\ a_{44} \end{bmatrix} \tag{1.5}$$

A matrisi kullanılarak, GDOP, PDOP (position dilution of precision), HDOP (horizontal dilution of precision) hesapları sırasıyla Eşitlik (1.6), Eşitlik (1.7) Eşitlik (1.8)'de belirtildiği gibi yapılmaktadır [16].

$$GDOP = \sqrt{a_{11} + a_{22} + a_{33} + a_{44}} \quad (1.6)$$

$$PDOP = \sqrt{a_{11} + a_{22} + a_{33}} \quad (1.7)$$

$$HDOP = \sqrt{a_{11} + a_{22}} \quad (1.8)$$

Alıcılarda, küresel konumlama sistemlerinin sundukları 1-sigma (1-σ) pozisyon çözümü doğrulukları; kullanıcı eşdeğer aralık hatası (user equivalent range error, UERE) ve hassasiyet seyreltilmesi (dilution of precision, DOP) değerlerine bağlı olup, aşağıdaki Eşitlik (1.9)'da verildiği gibi hesaplanmaktadır.

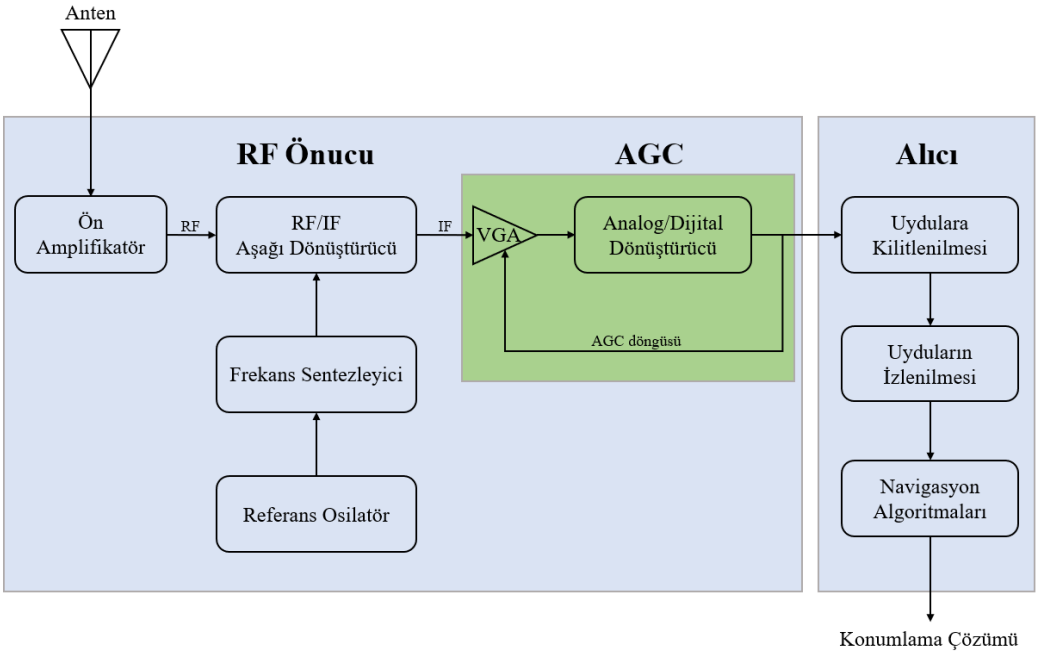
$$Pozisyon\ Doğruluğu = UERE * DOP \quad (1.9)$$

Burada, UERE; alıcı gürültüsü, iyonosferik ve troposferik gecikmeler, uydu efemeris hataları, uydu saat hataları, çoklu yol (multipath) etkisi gibi hata kaynaklarına bağlıdır [17].

1.2.3 Tipik KKS alıcısı yapısı

Basit bir KKS alıcısı yapısı Şekil 1.1'de verilmiştir. KKS uydularından gelen RF sinyaller, RF anteni tarafından alınmaktadır. Bu RF sinyalleri, düşük gürültülü bir ön yükselteç (pre-amplifier) tarafından yükseltilmektedir. RF ön ucuna (RF frontend) ulaşan bu yükseltilmiş RF sinyalleri, yerel osilatörlerden gelen sinyal karıştırma frekansları kullanılarak, aşağı-dönüştürücü (down-converter) bloğu ile analog IF sinyale dönüştürülmektedir. Yerel osilatörler, alıcı tasarımının frekans planına dayalı olarak frekans sentezleyici tarafından referans osilatörden üretilmektedir. Analog IF sinyalin dijital IF sinyaline çevrilebilmesi için analog-dijital çevirici kullanılmaktadır. Tüm KKS alıcı yapılarında olmamakla birlikte, özellikle aldatma saldırısı gibi anomali

tespiti için de kullanılan, geri beslemeli otomatik kazanç kontrolü (automatic gain control, AGC) bloğu da yer almaktadır. Analog-dijital çeviricinin çıktısı olan IF sinyaller, alıcı yapısının dijital alıcı kanallarına iletilmektedir. Bu kanallarda KKS uydularına kilitlenebilmek ve uyduları izleyebilmek için geliştirilen dijital sinyal işleme aşamaları yer almaktadır. Uydulardan alınan ölçümlerin işlenmesi ile elde edilen veriler, pozisyon-hız-zaman bilgisi üretilerek kullanıcıya sunulması amacıyla navigasyon algoritmalarından geçmektedir [2, 18].



Şekil 1.1: Tipik bir KKS alıcısı yapısı

1.2.4 Küresel konumlama sistemleri ölçümlerinde olası hata kaynakları

KKS alıcılarında kullanıcı konumunun hassas olarak belirlenmesindeki olası hatalar; ortam, uydu yörüngesi ve saat hatalarından, kullanıcı ekipmanlarından kaynaklanabilmektedir. Genel olarak;

- KKS uydularında oldukça hassas atomik saatler kullanılmasına rağmen; uydu saati hataları, konumlama çözümündeki en büyük hata kaynaklarındandır. Bu hataları azaltabilmek amacıyla, uydu saati hataları kontrol bölgelerinde sürekli olarak izlenmekte ve saat düzeltme parametreleri düzenli olarak navigasyon mesajı içerisinde yayınlanmaktadır [19].

- Uyduların yayınladığı navigasyon mesajları içerisindeki uydu konum bilgilerinin doğruluğundaki hataya uydu efemeris hatası denilmektedir [3]. Öngörülebilmesi ve modellenebilmesi zor olan hata kaynaklarından birisidir [20].
- İyonosferik ve troposferik hatalar da Dünya'nın atmosferik tabakalarından kaynaklanan hatalardandır. İyonosfer, KKS sinyallerinin atmosfere ulaştığında geçtiği ilk tabakadır. İyonosferde iyonlaşma ve serbest iyon yoğunluğu Güneş ışımalarına bağlı olarak sürekli değişkendir. Klobuchar, NeQuick G gibi farklı iyonosferik modellemeler ile benzetimleri yapılarak, iyonosferik düzeltmelerin yapılması sağlanabilmektedir [3, 20, 21]. Troposfer ise atmosferin en alt tabakasıdır. Troposferik hatalar; sıcaklık, basınç, nem, rüzgar gibi meteorolojik etkenlere, alıcıların uydular ile arasındaki açıya, sinyallerin troposferde kat ettikleri yola bağlı olarak oluşabilmektedir [20]. Saastamoinen, Hopfield, Goad & Goodman gibi modellemeler ile troposferik etkiler hesaplanmakta ve pozisyon çözümünün iyileştirilmesi sağlanmaktadır [22].
- KKS alıcısına gelen sinyaller, doğrudan uydulardan gelebileceği gibi, yeryüzünde çeşitli pek çok noktadan yansıyarak da ulaşabilmektedir. Sinyallerin, yansıyarak bir veya birden fazla yol izlemesine ve yansımadan doğrudan iletilen sinyalle birlikte alıcı antenine ulaşmasına çoklu yol (multipath) etkisi denilmektedir. Çoklu yol etkisinin tahmin edilebilmesi ve sebep olduğu ölçüm hatalarının azaltılabilmesi için çeşitli yöntemler literatürde yer almaktadır [23, 24].
- KKS alıcılarının termal gürültüsü, anten gürültüsü gibi sistem gürültüleri [25] ve pozisyon hesabında kullanılan yöntemlerin hassasiyeti de ölçüm hatalarına sebep olabilmektedir [3, 26].
- Aldatma saldırılarına uğrayan bir KKS alıcısının da pozisyon ölçümlerinde yüksek hatalar oluşmaktadır. Aldatıcı sinyaller üreten kaynağın amacı; hedef alıcının kendini farklı bir konumda zannetmesi olduğundan, alıcının içerisinde başarılı bir şekilde çalışan aldatmaya karşı önlem algoritmaları olmadığı takdirde, oldukça hatalı sonuçlar gözlemlenebilmektedir.

1.2.5 Ataletsel ölçüm birimi ve olası hata kaynakları

Ataletsel ölçüm birimi (AÖB / Inertial measurement unit, IMU) ivmeölçer ve dönüölçer birimlerinden oluşmaktadır. AÖB'nin amacı; ivmeölçeri ile ivme verisi, dönüölçeri ile de açısal hız verisini üç eksende ölçmektir. Kullanım alanına göre, farklı hassasiyette sensörlere sahip AÖB'ler bulunmaktadır. Özellikle MEMS (micro elektro-mechanical systems) AÖB sensörler, düşük maliyetli, küçük boyutlu, kolay erişilebilir, hızlı entegre edilip uygulanabilir olması gibi özellikleri bakımından pek çok uygulama alanında yaygın olarak kullanılmaktadır. İvmeölçer ve dönüölçere ait ilk değerler bilindiğinde, bu sensör ölçümlerinin integralinin alınması yöntemi ile doğrusal hız ve açısal değişim hesaplanabilmektedir [27].

İvmeöçer ve dönüölçer sensörlerinin hataları; deterministik ve stokastik (olasılıksal) olmak üzere iki farklı tür hatadan kaynaklanmaktadır. Deterministik hatalar; ataletsel sensörlerin kullanımı sırasında gözlemlenerek düzeltilebilecek hatalardır. Öte yandan, stokastik hataların tespit edilip giderilebilmesi çok daha zorludur.

Temel olarak deterministik hatalar; sabit kayma (bias), orantı katsayısı (scale factor), eksen kaçıklığı (misalignment) kaynaklı olabilmektedir. Stokastik hatalar; nicemleme (quantization), rastgele yürüyüş (random walk) kaynaklı olabilmektedir [27-30].

Deterministik hatalar

- Sabit kayma hatası; sensörlerin ölçüm çıktılarında herhangi bir girdi olmadığı durumda gözlemlenen sinyalin ortalama değeridir. Ataletsel sensörlerin her biri için, üç eksende de farklı değerlerde olabilecek olup, uygulamaya başlangıç öncesinde gözlemlenip offset olarak eklenmesi ile giderilebilmektedir. Birimi ivmeölçer için m/s^2, dönüölçer için drc/s'dir.

- Orantı katsayısı hatası; ivmeölçer ve dönüölçerlerin çıkış ve giriş sinyalleri arasındaki oranın 1 değerinden farkını ifade etmektedir. Birimi yüzde (%) veya ppm'dir.

- Eksen kaçıklığı hatası; sensörlerin birbirlerine tam olarak dik eksenlere yerleştirilememesinden kaynaklanabilecek bir hatadır. Hassas montaj ve kalibrasyon ile bu hatalar olabildiğince önlenebilmektedir. Birimi mrad'dır.

Stokastik hatalar

- Nicemleme hatası; analog sensör ölçümlerinin dijitale çevirilmesi sırasında, sensörlerin analog-dijital çeviricisinin bit çözünürlük hassasiyetine bağlı olarak oluşan bir hata türüdür. Olabildiğince hassas çevirici kullanılarak nicemleme hataları azaltılabilmektedir.

- Rastgele yürüyüş hatası; ataletsel sensörlerin termo-mekanik bozucu etkenlerden kaynaklanan hatalarını ifade etmekte olup, beyaz gürültü olarak tanımlanmaktadır. Ataletsel sensörler için en baskın etkiye sahip hata türüdür. Bu hatanın etkisinin azaltılabilmesi için alçak geçirgen filtre kullanılabilmektedir.

1.2.6 Ataletsel ölçüm birimi modellemesi

Tipik bir AÖB modellemesi, üç eksendeki ivme ve dönü ölçümlerinin gerçek değerlerine, olası hata bileşenlerinin de eklenmesi ile ifade edilebilmektedir. Sırasıyla ivmeölçer ve dönüölçeri tanımlayan eşitlikler olmak üzere, Eşitlik (1.10) ve Eşitlik (1.11)'de verilen matrisler ile modellenebilmektedir [27].

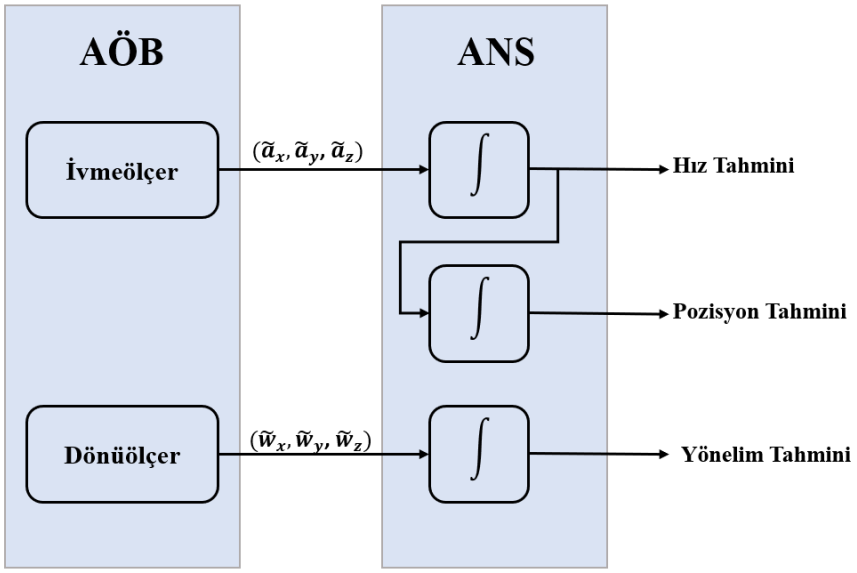
$$\begin{bmatrix} \tilde{a}_x \\ \tilde{a}_y \\ \tilde{a}_z \end{bmatrix} = \begin{bmatrix} 1+S_x & M_{xy} & M_{xz} \\ M_{yx} & 1+S_y & M_{yz} \\ M_{zx} & M_{zy} & 1+S_z \end{bmatrix} \begin{bmatrix} a_x \\ a_y \\ a_z \end{bmatrix} + \begin{bmatrix} B_x \\ B_y \\ B_z \end{bmatrix} + \begin{bmatrix} \eta_x \\ \eta_y \\ \eta_z \end{bmatrix} \tag{1.10}$$

$$\begin{bmatrix}\tilde{w}_x\\ \tilde{w}_y\\ \tilde{w}_z\end{bmatrix} = \begin{bmatrix}1+S_x & M_{xy} & M_{xz}\\ M_{yx} & 1+S_y & M_{yz}\\ M_{zx} & M_{zy} & 1+S_z\end{bmatrix}\begin{bmatrix}w_x\\ w_y\\ w_z\end{bmatrix} + \begin{bmatrix}B_x\\ B_y\\ B_z\end{bmatrix} + \begin{bmatrix}B_{gx} & 0 & 0\\ 0 & B_{gy} & 0\\ 0 & 0 & B_{gz}\end{bmatrix}\begin{bmatrix}a_x\\ a_y\\ a_z\end{bmatrix} + \begin{bmatrix}\eta_x\\ \eta_y\\ \eta_z\end{bmatrix} \quad (1.11)$$

$\tilde{a}_x, \tilde{a}_y, \tilde{a}_z$ ve $\tilde{w}_x, \tilde{w}_y, \tilde{w}_z$ ifadeleri sırasıyla ivmeölçer ve dönüölçer için ölçülen üç eksendeki sensör değerlerini ifade etmektedir. a_x, a_y, a_z ve w_x, w_y, w_z ifadeleri ise sırasıyla ivmeölçer ve dönüölçer için üç eksendeki gerçek ivme ve dönü değerleridir. S_x, S_y, S_z değerleri orantı katsayı hatalarını, B_x, B_y, B_z değerleri sabit kayma hatalarını, η_x, η_y, η_z değerleri stokastik hataları, $M_{xy}, M_{xz}, M_{yx}, M_{yz}, M_{zx}, M_{zy}$ ifadeleri eksen kaçıklığı hatalarını temsil etmektedir.

1.2.7 Ataletsel navigasyon sistemi modellemesi

Hareketli bir araç üzerindeki AÖB sensörlerinden alınan ivme ve dönü ölçümleri ile pozisyon, hız ve yönelim tahminlerinin hesaplanmasına ataletsel navigasyon sistemi (ANS / inertial navigation system, INS) denilmektedir. Temel olarak; ivmeölçerden anlık olarak elde edilen ivme tahminlerinin, ANS tarafından bir kez integralinin alınması ile hız tahminleri, bir kez daha integralinin daha alınması ile de pozisyon tahminleri elde edilebilmektedir. Dönüölçerin gelen dönü tahminlerinin integre edilmesi ile de yönelim açısı tahmini yapılmaktadır. Bununla beraber, farklı eksen takımları için farklı mekanizasyon denklemleri uygulanarak ANS çözümü elde edilebilmektedir. Basit bir AÖB ve ANS yapısı Şekil 1.2'de verilmiştir. ANS'nin en temel dezavantajı zamanla hata biriktiren bir sistem olmasıdır [31].



Şekil 1.2: AÖB ile ANS blok şeması

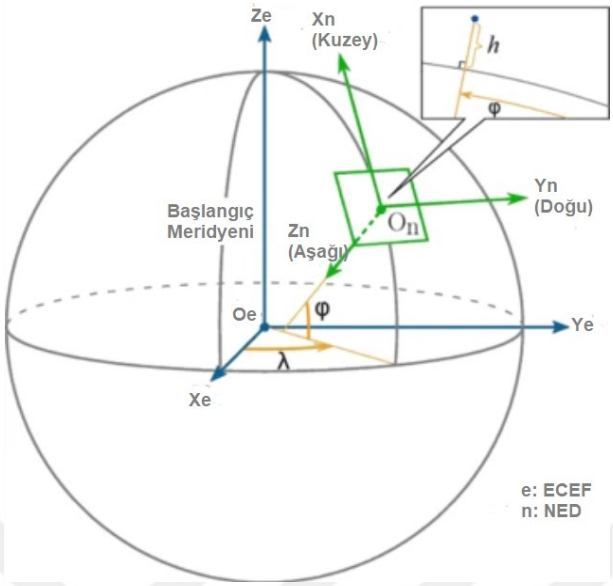
1.2.8 Kuzey-doğu-aşağı (NED) ve yer merkezli-yer sabit (ECEF) koordinat sistemleri

Herhangi bir nesnenin pozisyonunu, hızını ve yönelimini (orientation) belirtebilmek için uygun bir koordinat sisteminde tanımlamak gerekmektedir. Amaca yönelik olarak çeşitli koordinat sistemleri kullanılabilmekte olup, bu tez kapsamında aşağıdaki koordinat sistemleri ile çalışılmıştır.

Kuzey-doğu-aşağı (NED) koordinat sistemi; Dünya yüzeyine sabit olup, nesnenin jeodezik kuzey, doğu ve negatif yönde yükseklik bilgileri ile tanımlanmaktadır. Kuzey ve doğu için birimleri derece (°), aşağı için ise metre (m) olarak kullanılmaktadır.

Yer-merkezli yer-sabit koordinat sistemi; Dünya'nın kitle merkezini başlangıç noktası olarak almakta ve nesnenin bu merkez noktasına göre, x-y-z eksenlerindeki metre cinsinden uzaklıkları olarak tanımlanmaktadır. Bu koordinat sistemleri, Dünya'nın dönmesi ile de sürekli olarak hareket etmektedir.

NED ve ECEF Koordinat Sistemleri Şekil 1.3‘te verildiği gibi görselleştirilmektedir [32].



Şekil 1.3: NED ve ECEF koordinat sistemleri

Şekil 1.3’te mavi renk ile eksenleri gösterilen ECEF, yeşil renk ile gösterilen ise NED koordinat sistemidir. NED için tanımlanan noktayı ifade etmede kullanılan λ değeri başlangıç meridyeninden olan açısal uzaklığı (boylam), φ ise Ekvator’a olan açısal uzaklığı (enlem) belirtmektedir.

NED koordinat sisteminden ECEF koordinat sistemine geçiş için kullanılan $D_{N/E}$ dönüşüm matrisi Eşitlik (1.12)’te verilmiştir [32].

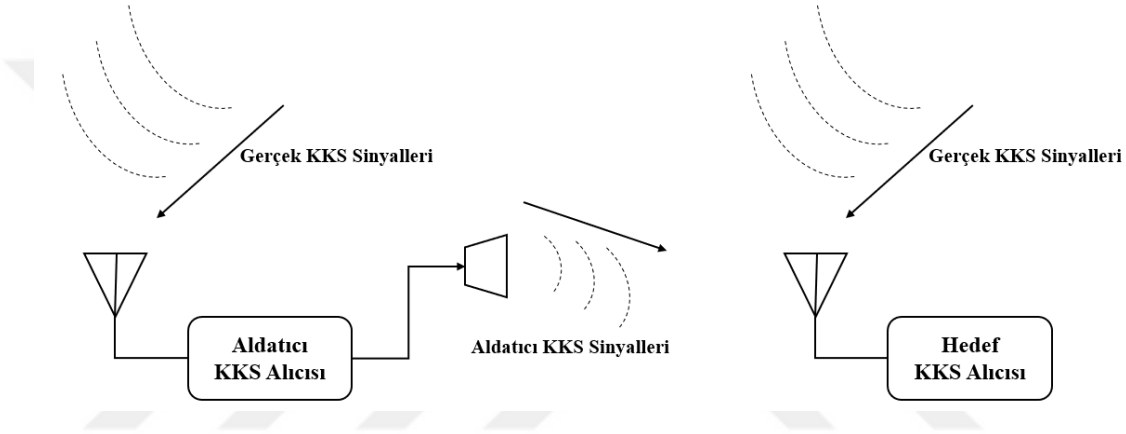
$$D_{N/E} = \begin{bmatrix} -sin\varphi_{ref}cos\lambda_{ref} & -sin\varphi_{ref}sin\lambda_{ref} & cos\varphi_{ref} \\ -sin\lambda_{ref} & cos\lambda_{ref} & 0 \\ -cos\varphi_{ref}cos\lambda_{ref} & -cos\varphi_{ref}sin\lambda_{ref} & -sin\varphi_{ref} \end{bmatrix} \quad (1.12)$$

ECEF koordinat sisteminden NED’e geçiş için kullanılan $D_{E/N}$ dönüşüm matrisi ise Eşitlik (1.13)’teki gibi hesaplanmakta olup, Eşitlik (1.12)’deki ifadenin tersine ve transpozuna eşit olmaktadır.

$$D_{E/N} = {D_{N/E}}^{-1} = {D_{N/E}}^{T} \quad (1.13)$$

1.2.9 Tipik aldatma saldırıları

Tipik bir aldatma saldırısı blok diyagramı Şekil 1.4'te verildiği gibidir [33]. Aldatıcı sinyal üreten KKS alıcısı, gerçek KKS sinyallerini alarak aldatıcı sinyalleri üretmekte ve hedef alıcıya doğru yeniden yollamaktadır. Hedef alıcı da hem gerçek hem de aldatıcı sinyalleri almaktadır. Uygulanan aldatma yönteminin başarımına ve hedef alıcının içindeki aldatmaya karşı tedbir algoritmalarının performansına bağlı olarak, hedef alıcının aldatılması sağlanabilmektedir.



Şekil 1.4: Aldatma blok diyagramı

Genellikle, aldatma saldırılarında hedef olarak KKS kullanarak navigasyon yapan insansız hava, kara, deniz araçları tercih edilmektedir. İnsansız araçların hedef seçilmesindeki temel etken, insan kontrolündeki araçlarda konum ve yönelim değişimlerinin insanlar tarafından da gözlemlenebilmesi ve olası aldatma saldırıların kolaylıkla fark edilebilir olmasıdır.

Son yıllarda, aldatma saldırıları uygulamaları yaygınlaşarak raporlanmaya başlamıştır. Örneğin, 2011 yılında, Amerikalılara ait bir insansız hava aracı İran tarafından GPS aldatması uygulanarak ele geçirilmiştir [34]. 2017'de raporlandığı üzere, Karadeniz'de birçok defa aldatma saldırıları gözlenmiştir [35].

1.2.10 Aldatma saldırıları tespit ve karşı tedbir yöntemleri

Literatürde aldatma saldırılarının tespit ve karşı önlemlerine dair çeşitli yöntemler yer almaktadır.

- KKS alıcılarında aldatma saldırısı tespit edebilmenin temel yöntemlerinden biri; alıcıda alınan KKS sinyalin güç seviyesini incelemektir. Başarılı bir aldatma saldırısı yapabilmek amacıyla, gerçek KKS sinyallerinden daha yüksek güç seviyelerinde sinyal üreten aldatıcılar, hedef alıcılarda daha yüksek mutlak güç alınmasına sebep olabilmektedir. Dolayısıyla, mutlak gücün sürekli olarak takip edilmesi ve beklenenden yüksek seviyelerde gözlenmesi ile aldatma saldırısı tespiti yapılabilmektedir [36, 37].
- Benzer bir başka aldatma tespiti yöntemi; taşıyıcı-gürültü oranının (carrier-to-noise ratio, C/N_0) incelenmesidir. Aldatıcıdan alınan sinyal gücü genellikle gerçek KKS uydularından alınan sinyal gücünden yüksek seviyelerde olmaktadır. Dolayısıyla, alıcılarda sürekli olarak C/N_0 seviyesinin takip edilmesi ve ani bir yükselişin gözlenmesi sayesinde aldatma tespiti yapılabilmektedir [36].
- GPS özelinde kullanılan bir diğer aldatma tespit yöntemi de farklı frekans bantlarında (L1 ve L2) yayın yapan GPS sinyallerinin güç seviyelerinin karşılaştırılmasıdır. Genellikle, çoğu KKS alıcısı L1 ve L2 frekans bantlarına uyumlu olmasına rağmen, çoğu aldatıcı sadece L1 frekansından aldatma sinyali üretebilmektedir. Dolayısıyla, alıcıda bu frekans bantlarının güç seviyeleri arasındaki fark artmakta ve aldatmanın tespit edilebilmesi sağlanmaktadır [33, 36].
- Sinyal varış açısı tespiti (Signal angle of arrival detection) yöntemi; aldatıcı sinyaller ile gerçek KKS sinyallerinin hedef alıcıya farklı açılarla varması esasına dayanmaktadır. Aldatma sinyali tespiti başarımı oldukça yüksek olmasına rağmen, alıcıda çoklu anten gereksinimi kullanım alanını kısıtlamaktadır. [36]
- PRN kodu ve data bitlerindeki gecikmeler sayesinde de aldatma sinyali tespiti yapılabilmektedir. Gerçek KKS uydu sinyallerini alıp çözümleyerek aldatma sinyali üreten bir aldatıcının sinyalleri, gerçek sinyallere kıyasla bir miktar

gecikme ile hedef alıcıya ulaşmaktadır. Bu zaman gecikmesinin alıcı tarafından tespit edilmesi yöntemi ile de aldatma saldırısı tespiti yapılabilmektedir [33].

- Otomatik kazanç kontrolü (Automatic gain control, AGC) tespiti yöntemi ile, KKS alıcılarının RF ön ucunda aldatma sinyali tespiti yapılabilmektedir. AGC; RF ön uçtaki kazancın analogdan dijitale dönüştürücünün (analog-to-digital converter, ADC) giriş aralığına göre optimize etmek için kullanılmaktadır [18]. KKS alıcılarında, alınan sinyal gücü termal gürültünün altında kalmaktadır ve radyo frekans girişimi (radio frequency interference, RFI) nedeniyle oldukça değişken değerlerdedir. KKS alıcısı ön ucundaki sinyalin ADC'ye optimum ve sabit bir güç ile, istenilen bant genişliğinde gelebilmesini sağlayabilmek için AGC döngüsünden faydalanılmaktadır [38, 39].

  Gürültü gücünün uydu sinyalleri gücünden çok daha yüksek olduğu bilindiği için, herhangi bir aldatma saldırısı olması durumunda AGC'de hızlı bir azalma gözlenmekte ve bu anormalliğin tespit edilmesi ile aldatma saldırısı tespiti yapılabilmektedir [36, 40].

- Sinyal kalitesi izlenmesi (Signal quality monitoring, SQM) yöntemi ise; gerçek uydu sinyalleri ile aldatma sinyallerinin korelasyonunun incelendiğinde, korelasyon tepe noktasında bozulmanın tespit edilmesi esasına dayanmaktadır. Ortamda herhangi bir aldatma sinyali yokken, sinyallerin korelasyonu üçgen şeklinde elde edilmektedir. Aldatıcı sinyalin olması durumunda ise, üçgen şeklindeki korelasyon tepe noktası bozulmakta ve dolayısıyla aldatma sinyali tespit edilebilmektedir [33, 36].

- Aldatma tespiti için kullanılan yöntemlerden bir diğeri ise, doppler frekansı ile kod gecikme hızlarının incelenmesidir. Aldatma sinyallerinin olmadığı bir ortamda, gerçek KKS sinyallerinin doppler frekansı ile kod gecikme hızı ilişkili olup, ikisi de KKS uyduları ile alıcı arasındaki bağıl harekete bağlıdır. Bu nedenle, hedef alıcıda yer alan faz kilitli döngünün (phase locked loop, PLL) ve gecikme kilitli döngünün (delay locked loop, DLL) çıkışları tutarlı değilse, aldatma sinyali tespiti yapıldığı söylenebilmektedir [33].

- Hedef alıcıya gelen efemeris bilgilerinin kontrolü ile de aldatma tespiti yapılabilmektedir. Her KKS uydusu, sürekli olarak efemeris yayını ile

uyduların yörüngedeki pozisyon ve hız bilgilerini yayınlamaktadır. Bu yayınlarda tespit edilebilecek bir tutarsız da aldatma saldırısı tespiti kararında kullanılabilmektedir [33].

- Alıcı otonom bütünlük izlenmesi (Receiver autonomous integrity monitoring, RAIM) yöntemi; alıcılarda hatalı sözde menzil (pseudo range) ölçümlerinin belirlenerek tutarlılığın sağlanmasını amacıyla yaygın olarak kullanılmaktadır [36, 41, 42]. KKS sinyallerinde uzamsal tutarlılıklarının kontrol edilerek, anormallik tespit edilen sinyallerin hariç tutulması esasına dayalı olan bu yöntem, aldatma saldırısı tespiti ve aldatmaya karşı önlem kapsamında da kullanılmaktadır. Ancak, sadece bir veya iki aldatıcı sinyalin bulunduğu koşullarda uygulanabilir bir yöntem olması da dezavantajıdır. [36]
- Hedef alıcıda çoklu KKS uyduları kullanılarak pozisyon çözümü yapılması ile, herhangi bir konumlandırma sistemi üzerinden uygulanan aldatma saldırısının tespit edilebilmesi sağlanabilmektedir. Dolayısıyla, olabildiğince çoklu KKS uyduları ile konumlama hesabının yapılması, sağlıklı çözüm elde edilmesi ihtimalini arttırmaktadır. Alıcıda gözlemlenen uyduların konumlarına göre, hatalı veriye sahip olan ve olmayan uydular kümeleri oluşturulması, olası hatalı uyduların elenerek sağlıklı veriye sahip uydu sinyalleri ile pozisyon hesabı yapılması yöntemi de bu kapsamda literatürde önerilmektedir [43].
- KKS alıcılarına karşı uygulanan bir aldatma saldırısının tespiti için kullanılabilecek temel yöntemlerden biri de; ivmeölçer, AÖB (IMU), odometre, pusula, kamera, LiDAR gibi ek sensörlerin sisteme entegre edilerek pozisyon çözümünün kontrol edilip iyileştirilmesidir [33, 44, 45, 46]. Diğer sensörlerden gelen veriler ile olası anormallikler ya da saldırılar tespit edilebilmekte ve gerekli karşı tedbirlerin alınması sağlanabilmektedir [47].

1.2.11 Kalman filtresi hakkında genel bilgiler

Kalman filtresi 1960'lı yıllardan beri, navigasyon alanında başta olmak üzere pek çok alanda, oldukça yaygın olarak araştırma ve uygulama konusu olmuştur. Filtrenin temel amacı; sistemin durumlarının optimal olarak tahmin edilebilmesidir ve bunun için yinelemeli bir dizi matematiksel denklemden faydalanmaktadır [48].

Filtre temel olarak; sistem modeli, ölçüm modeli ve hata kovaryansından oluşmaktadır. Sistem modeli, filtre değişkenleri ile hata kovaryansı arasındaki ilişkiyi, ölçüm modeli, ölçümler ile durum değişkenleri arasındaki ilişkiyi yansıtmaktadır. Hata kovaryansları ise durum tahminleri ile ölçümler arasındaki belirsizliği ifade etmektedir [27].

Ayrık zamanlı bir Kalman filtresinde sistem modeli Eşitlik (1.14)'te, ölçüm modeli Eşitlik (1.15)'te verildiği gibi ifade edilebilmektedir [27].

$$x_k = Fx_{k-1} + Bu_{k-1} + n_{k-1} \tag{1.14}$$

$$z_k = Hx_k + v_k \tag{1.15}$$

x_k ve z_k ifadeleri, sırasıyla, k zaman adımındaki durum ve ölçümleri tanımlamaktadır. $(k-1)$ alt indisi, filtrenin bir önceki zaman adımından gelen ifadeler olduğu anlamına gelmektedir. F, durum dönüşüm matrisi olup durum vektörünün zamana bağlı ilişkisini yansıtmaktadır. u vektörü kontrol girdisi olup, B matrisi kontrol girdisi ile sistem arasındaki geçişi belirtmektedir. Ölçüm modelinde kullanılan H matrisi, gözlem matrisi olup sistem ile ölçüm arasındaki ilişkiyi yansıtmaktadır. n_k ve v_k ifadeleri, 0 ortalamalı ve sırasıyla Q ve R varyanslı gürültü bileşenleridir. Q durum hata kovaryansı, R ise ölçüm gürültü kovaryansı vektörü olup, sırasıyla durum ve ölçüm sayısı boyutlulardır.

Filtre, durum vektörü ve hata kovaryans matrisinin ilklendirilmesi ile başlamaktadır.

Kalman filtresi; zaman güncellemesi (tahmin) ve ölçüm güncellemesi (düzeltme) aşamalarından oluşmaktadır. Bu aşamaların çıktıları, birbirlerini besleyen denklemlerden oluşmaktadır. Zaman ve ölçüm güncellemesi aşamalarının denklemleri ve detayları aşağıda anlatılmaktadır [27, 48].

Zaman Güncellemesi

Zaman güncellemesi denklemleri Eşitlik (1.16) ve Eşitlik (1.17)'de verildiği gibi tanımlanmakta olup, bu denklemler ile sistemin bir sonraki filtre zaman adımındaki durum ve hata kovaryansı tahminleri yapılmaktadır.

$$\hat{x}_k^- = F\hat{x}_{k-1} + Bu_{k-1} \tag{1.16}$$

$$P_k^- = FP_{k-1}F^T + Q \tag{1.17}$$

Bu eşitliklerdeki $\hat{x}_k^-$ ve P_k^- ifadeleri, sırasıyla anlık durum ve hata kovaryansı tahminlerini belirtmektedir. $\hat{x}_{k-1}$ ve P_{k-1} ifadeleri, ölçüm güncellemesi aşamasında hesaplanarak geri beslenen durum ve hata kovaryansı değerleridir. Q durum hata kovaryansı matrisi olup durum sayısı boyutlu bir kare matristir.

Ölçüm Güncellemesi

Ölçüm güncellemesi aşamasında, zaman güncellemesi aşamasından gelen hata kovaryansı kullanılarak Kalman kazancı hesaplanmaktadır. Gelen anlık ölçümler, Kalman kazancı ve zaman güncellemesinde hesaplanan durum tahminleri kullanılarak

durum kestirimleri yapılmaktadır. Ardından hata kovaryansı, hesaplanan Kalman kazancı ile güncellenerek zaman güncellemesi aşamasını tekrar beslemektedir.

Kalman kazancı hesabı, durum kestirimi ve hata kovaryansı güncelleme adımları sırasıyla Eşitlik (1.18), Eşitlik (1.19) ve Eşitlik (1.20) denklemleri ile tanımlanmaktadır.

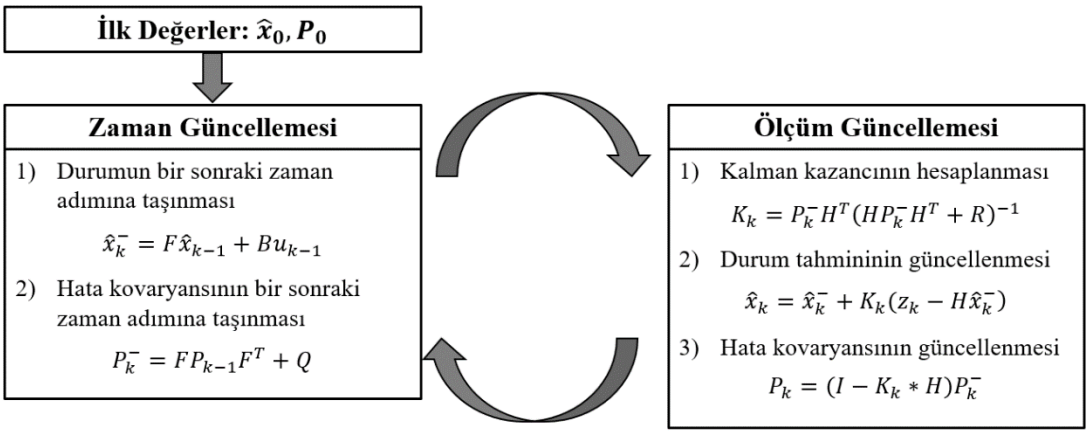
$$K_k = P_k^- H^T (H P_k^- H^T + R)^{-1} \tag{1.18}$$

$$\hat{x}_k = \hat{x}_k^- + K_k (z_k - H\hat{x}_k^-) \tag{1.19}$$

$$P_k = (I - K_k * H) P_k^- \tag{1.20}$$

Yukarıdaki eşitliklerdeki K_k, $\hat{x}_k$ ve P_k ifadeleri, sırasıyla Kalman kazancı, durum tahmini ve hesaplanan hata kovaryansını belirtmektedir. *H* gözlem matrisi, *R* ise ölçüm hatası kovaryans matrisidir. z_k ifadesi anlık olarak gelen ölçüm girdilerini temsil etmektedir. *I* ise birim matristir.

Temel bir Kalman filtresi diyagramı Şekil 1.5'te özetlendiği gibidir [49].



Şekil 1.5: Kalman filtresi diyagramı

1.2.12 Kalman filtresi ile KKS ve AÖB tümleşimi yöntemleri

KKS ve AÖB ölçümleri, doğaları gereği belirli bir doğrulukta ve farklı hatalar ile konumlama bilgisi sunabilmektedir. Dolayısıyla bu sistemlerden gelen verileri birleştirerek olası pozisyon tahmini hatalarını azaltmaya oldukça yaygın olarak ihtiyaç duyulmuştur. Bu doğrultuda, Kalman filtresi ile farklı sistemlerden gelen bu ölçümlerin tümleşimini yapmak pek çok alanda çalışma konusu olmuştur.

Örneğin, [28] numaralı tez çalışmasında, KKS ve MEMS AÖB'nin farklı Kalman filtreleme yöntemleri ile tümleşimleri incelenmiştir. Sıkıca bağlı (tightly coupled) ve gevşek bağlı (loosely coupled) bütünleştirme teknikleri ile genişletilmiş Kalman filtresi (extended Kalman filter, EKF) ve kokusuz Kalman filtresi (unscented Kalman filter, UKF) algoritmaları ele alınmış ve performansları araç üzerinde yapılan testler ile değerlendirilmiştir. UKF hata tahmininin, KKS ölçümlerinde kayıplar olması koşulunda daha iyi sonuçlar sunabildiği; EKF'nin ise daha hassas bir şekilde yönelim açısı tahmini yapabildiği görülmüştür. Gevşek bağlı tümleşim yaklaşımına kıyasla, sıkıca bağlı yönteminin hem EKF hem de UKF mimarisi için daha başarılı sonuçlar verdiği gösterilmiştir.

Benzer olarak, [50] numaralı çalışmada, otonom bir hava aracı navigasyonu için GPS/ANS entegrasyonu için Kalman filtresi kullanılmıştır. Düşük maliyetli ve istenilen hassasiyette veri entegrasyonu sağlanabildiği için ideal bir kullanım uygulaması olduğu belirtilmiştir.

Öte yandan, KKS ve AÖB sistemlerine ek olarak, farklı sistemlerin de Kalman filtresi girdisi olarak kullanılması ile konumlama ve navigasyon performansları iyileştirilebilmektedir. Örneğin [51] numaralı referans bildiride, otonom bir kara aracı navigasyonu için GPS, fiber-optik dönüölçer, MEMS AÖB ve odometre ölçümlerinin Kalman filtresi ile entegrasyonu anlatılmaktadır. Sonuçlar, Kalman filtresi ile tümleşimi yapılan mimari sayesinde, doğruluğun ve gürbüzlüğün arttığını göstermektedir. GPS sinyallerinde kısa süreli kesintiler olsa dahi, filtrenin başarılı bir

şekilde konum tahmini üretmeye devam edebildiği de gösterilerek, otonom kara aracı navigasyonunda kullanılabilir olduğu vurgulanmıştır.

Benzer bir çalışma olarak, [52] referanslı bildiride, araç navigasyonu kapsamında GPS, ANS, odometre, eğimölçer sensörlerinin füzyonu ile pozisyon tahmini için KF, EKF, UKF gibi farklı filtreleme yöntemleri anlatılmıştır. Ayrıca, sensörlerden biri veya bir kısmının arızalı olduğunda sistemin başarımı incelenmiştir. Hatalı ölçümlerin tespit edilip elenmesine dayalı bir adaptif sensör füzyonu mimarisi önerilmiştir.

[53] referanslı makalede, çoklu küresel konumlama sistemi ile AÖB/odometre tümleşimi için sıkıca bağlı genişletilmiş Kalman filtresi yaklaşımı önerilmiştir. Odometre ölçümlerinin filtre girdisi olarak kullanılması ile KKS ölçümlerinin zayıf olduğu durumlarda da başarılı pozisyon ve hız çözümleri üretilebilmesi sağlanabildiği söylenmiştir. Araç navigasyonu süresince ölçüm hatalarının önemli ölçüde azaltıldığı gösterilmiştir.

Uygulama alanının amacına göre, sıkıca bağlı veya gevşek bağlı Kalman filtreleme yaklaşımlarından uygun olarak seçilen yöntem kullanılabilmektedir. Bu filtreleme yaklaşımlarının temel farkı, KKS alıcısının sağladığı hangi verinin filtre girdisi olarak belirlenmesindedir. Gevşek bağlı filtrelemede, uydulardan alınan sinyaller ile elde edilen sözde menzil ve doppler kayması bilgileri kullanılarak alıcı tarafında üretilen pozisyon ve hız tahminleri filtrenin birer girdisi olmaktadır. AÖB tarafından gelen ivme ve dönü ölçümlerinden sağlanan, ANS'nin pozisyon ve hız tahminleri de filtreye bir diğer girdi kaynağı olarak verilmektedir. Sıkıca bağlı bir filtreleme yaklaşımında ise, ANS'nin tahminlerine ek olarak, uydulardan elde edilen anlık sözde menzil ve doppler ölçümleri doğrudan filtre girdisi olarak sağlanmaktadır. Başka bir deyişle, sıkıca bağlı Kalman filtresinde ham KKS verileri filtreyi beslerken, gevşek bağlı Kalman filtresinde KKS alıcısının üretmiş olduğu pozisyon ve hız çözümleri kullanılmaktadır [54].

Gevşek bağlı filtrelemenin temel avantajlarından biri, AÖB veya KKS sistemlerinden birinin ölçüm vermemesi senaryosunda bile filtrenin çalışmaya devam edebilmesidir. Bir diğer avantajı ise, sıkıca bağlı filtrelemeye göre daha az sayıda durum kullanımı gerektirmesidir. Böylelikle, işlemlerde kullanılan matris boyutları da daha küçük olduğundan işlem hızı daha yüksek olmaktadır. Gevşek bağlı filtrelemenin, sıkıca

bağlıya kıyasla, doğrudan AÖB ve KKS alıcısı çıktılarını kullanması ile sistemdeki gürültünün daha yüksek seviyelerde olması ve Kalman filtresi çıkışındaki olası hataların daha yüksek seviyelerde olabilmesi ise dezavantajı olarak belirtilmektedir [28, 54].

1.2.13 KKS ve AÖB tümleşimi ile aldatma tespiti ve karşı tedbiri

KKS ve AÖB ölçümlerinin tümleşimi ile hassas konumlama yapılabilmesi, aldatma saldırılarının tespiti ve karşı önleminin alınabilmesi yöntemi olarak da literatürde çeşitli kaynaklarda ele alınmıştır.

Örneğin [44] numaralı bildiride, otonom bir araç navigasyonunda, aldatma tespiti ve karşı önlemi için GNSS alıcısına ek olarak AÖB ve odometre sensörlerinden gelen ölçümlerin füzyonu yapılmıştır. Bu çalışmada, KKS ve AÖB/odometre mekanizasyonu arasındaki tutarlılık kontrolüne dayalı bir aldatma algılama yaklaşımı önerilmiştir. Bir aldatma saldırısını tespit etmek için, yöntem önceden belirlenmiş bir gözlem penceresi sırasında KKS ve AÖB/odometre ölçümlerini bağımsız olarak analiz etmekte, KKS ve ANS/odometre mekanizması tarafından sağlanan çözümleri çapraz olarak kontrol etmektedir. Önerilen yöntemin performansı gerçek araç ortamlarında doğrulanmış, ortalama aldatma algılama süresi ve algılama performansı, farklı yoğunluklu ortamlarda incelenmiştir. GPS ile AÖB/odometreden gelen pozisyon vektörleri normu ile bu iki yörünge karşılaştırılmaktadır. Bu değer, önceden belirlenmiş bir eşik değerinin yüksekse aldatma saldırısı tespit edildiği söylenmektedir.

[55] numaralı referans bildiride, GPS ve GLONASS sistemlerinin Kalman filtresi ile füzyonu ele alınmış, ölçüm sonuçlarının güvenilirliği arttırılmaya çalışılmış, ardından GPS ile aldatma olduğu senaryosu altında test edilerek başarımı incelenmiştir. Burada filtre durumları, x-y-z eksenlerindeki pozisyon tahmin hataları, GPS ve GLONASS sistemlerinin zaman kayması hataları olacak şekilde tasarlanmıştır. GPS ile aldatma senaryoları üretilerek sözde menzil değişimlerinin gözlemlenmesi ve belli bir eşik değerinin aşılmasının denetlenmesi ile aldatma tespiti yapılmaya çalışılmıştır.

Aldatma tespit edilen sözde menzil ölçümlerine ait uydular elenerek geriye kalan görünür uydular ile pozisyon hesabı yapılmaya devam edilmektedir.

[56] numaralı bildiride ise, KKS alıcılarına yönelik aldatma saldırılarını tespit etmek için ANS ölçümlerini kullanan yeni bir dedektör önerilmektedir. Aldatma tespiti, sıkıca bağlı (tightly-coupled) bir ANS/KKS mekanizasyonunda Kalman filtresi inovasyonlarının izlenmesiyle gerçekleştirilmektedir. Monitörün performansı, Boeing747 uçak konumunu takip edebilen ve tahmin edilebilen aldatmanın varlığında değerlendirilmiştir. İniş yapan uçağın hedeflenen yörüngesi ve aldatıcının yönlendirmeyi çalıştığı hareket yörüngesi simülasyonlarla incelenerek performansı gözlenmiştir. Sensörlerin yüksek hassasiyete sahip olmadığı veya gecikme olmadığı sürece, önerilen dedektörün aldatma saldırılarını tespit etmek için etkili bir araç sağladığı gösterilmiştir.

ANS/KKS tümleşimi ile modellenmiş bir navigasyon sisteminin tümleşimi ve aldatma tespiti için Kalman filtresi tasarımı öneren, benzer bir başka çalışma da [57] numaralı bildiride sunulmuştur. Bu çalışmada, filtrenin ölçüm vektörü ANS ve KKS sistemlerinden gelen pozisyon çözümlerinin farkı olarak hesaplanmıştır. Kalman filtresi inovasyonuna dayalı aldatma tespiti metodu ele alınmıştır. Önerilen yöntem, inovasyon ve ölçümlerin ortalamalarını alarak, bu ortalama değerlerle hesaplanan kestirim hata kovaryans matrisini ki-kare (chi-squared) testinden geçirerek karşılaştırmaktadır. Geleneksel olarak kullanılan tek zaman pencereli yaklaşım ile, ölçümlerin belli bir zaman penceresinde birden fazla kere güncellenerek inovasyonların hesaplandığı ve ortalama inovasyon değerinin kullanıldığı yöntemler karşılaştırılmıştır. Ölçüm/inovasyon ortalaması alma yöntemlerinin aldatma saldırıları tespitinde daha başarılı olduğu sonucu çıkmıştır. Zaman adımları için zaman penceresi kullanılması ile, inovasyon ortalaması alma yönteminde küçük sapma büyüklüklerine sahip aldatma saldırıları daha yüksek başarım ile tespit edilebildiği görülmüştür.

[58] numaralı çalışmada, KKS alıcısına ek olarak kullanılan, çok döngülü ANS tahmini yoluyla gelişmiş bir inovasyon tabanlı aldatma dedektörü önerilmektedir. Her L döngüde genişletilmiş Kalman filtresi (EKF) ile düzeltilen ek bir ANS birimi eklenmektedir. Çıktısı, bir önceki aldatılmış tahminin yerini almak ve daha sonra geliştirilmiş bir inovasyon oluşturmak için kullanılmaktadır. Geleneksel inovasyon ile karşılaştırıldığında, geliştirilmiş inovasyon birden çok döngü boyunca aldatmaya karşı

bağışık olabilmekte ve aldatma saldırıları nedeniyle anormallik biriktirebilmektedir. Ek olarak, ani aldatma saldırılarını tahmin etmek için önceki inovasyonların ortalamalarını kullanarak yanlış alarm olasılığını azaltan bir yöntem sunulmuştur. Sonuçlar, önerilen aldatma tespit dedektörünün, yavaş değişen aldatma saldırıları altında tespit performansını önemli ölçüde iyileştirdiğini ve geleneksel dedektöre kıyasla yanlış alarm olasılığını azalttığını göstermektedir.

Benzer bir yaklaşımla, [59] numaralı bildiride, otonom bir araç için KKS, ivmeölçer, hızölçer, direksiyon açısı sensörü tümleşimi ile aldatma tespiti yöntemi önerilmektedir. Bu çalışmada, zaman serisine dayalı bir tahmin modeli kullanılmaktadır. Yapay özyinelemeli sinir ağı (artificial recurrent neural network/RNN) mimarisi, uzun kısa süreli bellek (long short-term memory, LSTM) kullanarak konum kaymasını ve kat edilen mesafeyi bir sonraki zaman damgası tarafından tahmin etmek için birden çok sensörden gelen verileri kullanmaktadır. Otonom araç tarafından tahmin edilen konum kayması herhangi bir aldatma saldırısını tespit etmek için, KKS tabanlı konum kaymasıyla karşılaştırılmaktadır. Ayrıca, dönüş algılama stratejisi ile, daha karmaşık aldatma saldırılarını da tespit etmek için aracın dönüşlerini sınıflandırma yöntemi önerilmiştir.

2. FARKLI KÜRESEL KONUMLAMA SİSTEMİ ÖLÇÜMLERİ İLE ALDATMA SALDIRISI TESPİTİ VE ALDATMAYA KARŞI ÖNLEM İÇİN KALMAN FİLTRESİ TASARIMI

2.1 Amaç

Literatürde KKS alıcılarında aldatma tespiti ve aldatmaya karşı önlem için farklı yöntemlerle önerilen çalışmalar bulunmaktadır. Tezin bu bölümünde, KKS alıcılarının pozisyonlama tahmini üretmeden hemen önceki navigasyon algoritmaları bloğunda kullanılmak üzere, aldatma tespiti ve aldatmaya karşı önlem almaya yönelik önerilen Kalman filtresi tasarımı yer almaktadır. Otonom bir kara aracı üzerine konumlandırılmış ve 4 farklı küresel konumlama sistemi uydu sinyallerini kullanarak pozisyonlama çözümü üreten bir KKS alıcısı kullanıldığı varsayılmıştır. 4 farklı sistemden elde edilen konumlama çözümü sonuçlarının tasarlanan Kalman filtresi yardımıyla birbirleri ile karşılaştırılarak aldatma tespiti yapılması, aldatma tespit edildiğinde de karşı önlem alınması hedeflenmektedir.

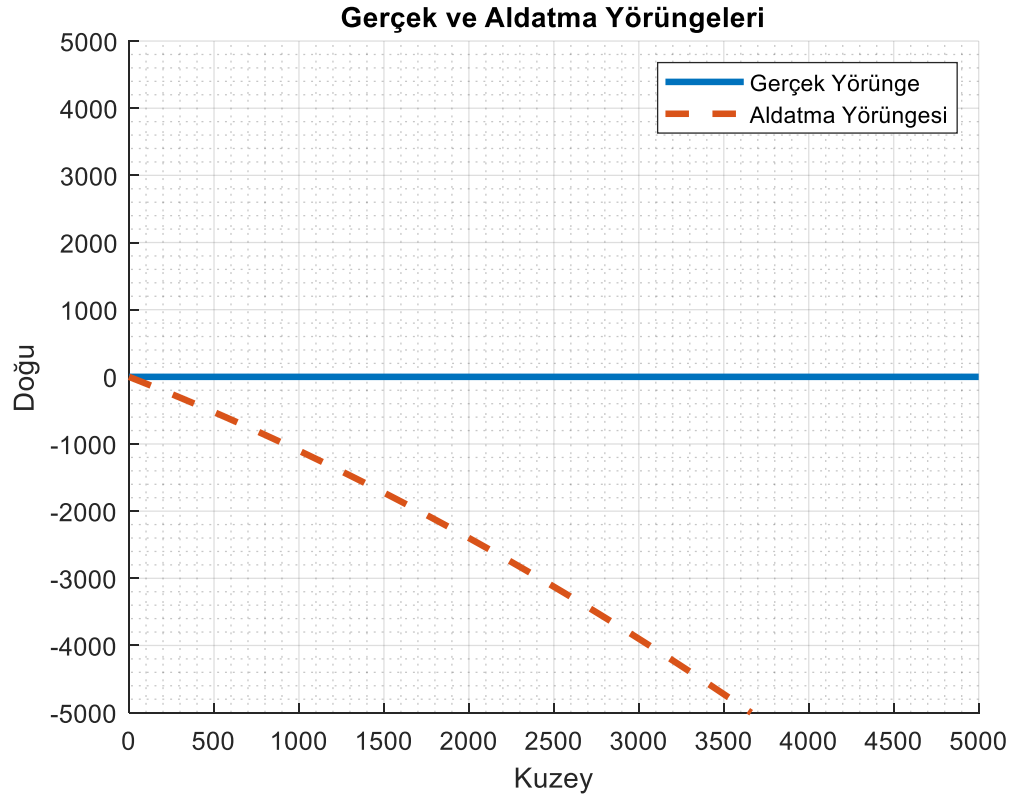
2.2 Algoritmanın Uygulanması

Bu bölümde; hareketli otonom bir aracı üzerinde yer alan, 4 farklı küresel konumlama sistemi kullanarak konumlama çözümü üreten bir KKS alıcısı için aldatma tespiti ve aldatmaya karşı önlem sunan bir Kalman filtresi yaklaşımı önerilmektedir. 4 farklı sistemi kullanarak elde edilen konumlama çözümünü çıktı olarak sunmadan önce kullanılmak üzere, aldatma saldırısı tespit performansını yükseltmek amacıyla tasarlanmıştır.

Bu kapsamda; öncelikle araç için gerçek ve aldatma hareket yörüngeleri modellenmiştir. Ardından, farklı çözüm doğrulukları ile küresel konumlama sistemleri çözümleri modellenmiştir. Son olarak, Kalman filtresi tasarımı ile bu ölçümler birleştirilmiş, aldatma tespit ve aldatmaya karşı önlem algoritması önerilmiştir.

2.2.1 Gerçek ve aldatma yörüngelerinin oluşturulması

Hareketli bir araç için gerçek hareket yörüngesi, belli bir başlangıç noktasından başlayacak ve simülasyon süresi boyunca kuzey yönüne doğru ilerleyecek şekilde, NED koordinat sisteminde oluşturulmuştur. Simülasyon süresi 1000 saniye, örnekleme zaman aralıkları 0.2 saniye olarak tanımlanmıştır. Oluşturulan bu gerçek hareket yörüngesine bağlı olarak, aracın gerçek yörüngeden ayrılmasını hedefleyecek şekilde bir aldatma hareketi yörüngesi oluşturulmuştur. Aldatma sinyali ürettiği modellenecek küresel konumlama sisteminin, bu aldatma yörüngesinde olacak şekilde konumlama çözümleri üreteceği varsayılmıştır. Gerçek ve aldatma hareketleri yörüngeleri Şekil 2.1'de görüldüğü gibidir.



Şekil 2.1: Gerçek ve aldatma hareket yörüngeleri

2.2.2 Küresel konumlama sistemi ölçümlerinin modellenmesi

KKS alıcısında konumlama çözümü sunabilmek için kullanılan 4 farklı küresel konumlama sistemi sırasıyla GPS, Galileo, GLONASS, BeiDou olacak şekilde tanımlanmıştır.

Bu sistemlerin sunduğu konumlama çözümleri, her saniyede bir üretilecek şekilde modellenmiştir [60]. Ayrıca, sistemler için tanımlanan yatay düzlemlerdeki sapma miktarları, tipik bir KKS alıcısının 1-sigma (1-σ) pozisyon doğruluklarına eşit olacak şekilde, Çizelge 2.1'de verildiği gibi tanımlanmıştır [61]. Bu değerler; zamana, konuma, ortam şartlarına ve alıcıya bağlı olarak değişken olup referansta verildiği doğrultuda tanımlanarak simülasyonlar gerçekleştirilmiştir.

Çizelge 2.1: Küresel konumlama sistemleri için yatay düzlemde konum sapma miktarları

Küresel Konumlama Sistemleri	**Yatay Düzlemde 1-σ Konum Sapma Miktarları (m)**
GPS	2.5
Galileo	3
GLONASS	4
BeiDou	3

2.2.3 Kalman filtresi tasarımı ve algoritmanın detayları

Bu bölümde, 4 farklı küresel konumlama sisteminden elde edilen konumlama çözümlerinin füzyonunu sağlamak, aldatma saldırısı tespiti yapabilmek ve aldatma varsa aldatmaya karşı tedbirin alınabilmesi amacıyla bir Kalman filtresi yaklaşımı sunulmaktadır.

Kalman filtresi başlangıç durumları Eşitlik (2.1)'de verildiği gibi tanımlanmıştır. Burada poz_x, poz_y, poz_z durumları yer merkezli-yer sabit (earth-centered earth-fixed, ECEF) koordinat sisteminde tanımlanmış 3-eksendeki başlangıç pozisyon değerleridir. 0 olarak ilklendirilmiş diğer üç durum ise, 3-eksendeki hız tahminleri için

oluşturulmuştur. Başlangıçta aracın hareketsiz olduğu varsayıldığı için 0 olarak tanımlanmıştır.

$$x_0 = \left[poz_x\ poz_y\ poz_z\ 0\ 0\ 0\right] \tag{2.1}$$

Filtrenin hata kovaryans matrisi P_k Eşitlik (2.2)'de verildiği gibi hesaplanmaktadır.

$$P_k^- = F\ P_{k-1}F^T + Q \tag{2.2}$$

Eşitlik (2.2)'deki; F durum dönüşüm matrisi, Q durum hata kovaryans matrisidir ve Eşitlik (2.3) ve Eşitlik (2.4)'te verildiği gibi oluşturulmuştur. Burada I birim matris, 0 sıfır matrisi, dt ise örnekleme zaman aralığı olup 0.2 saniye olarak belirlenmiştir.

$$F = \begin{bmatrix} I_{3x3} & dt * I_{3x3} \\ 0_{3x3} & I_{3x3} \end{bmatrix} \tag{2.3}$$

$$Q = 0.01 * I_{6x6} \tag{2.4}$$

Kalman kazancı K_k Eşitlik (2.5)'te verilen denklem ile hesaplanmaktadır. Bu eşitlikteki n ifadesi, KKS numarasını belirlemekte olup her KKS için Kalman kazancı ayrı ayrı hesaplanmaktadır.

$$K_{k,n} = P_k^- H^T (H P_k^- H^T + R_n)^{-1} \tag{2.5}$$

Eşitlik (2.5)'teki H gözlem matrisi, R ise ölçüm hata kovaryans matrisi olup Eşitlik (2.6) ve Eşitlik (2.7)'deki gibi tanımlanmıştır. Eşitlik (2.7)'deki $\sigma_{n,maks}$ ifadesi n'inci

KKS için tanımlanan maksimum pozisyonlama hatası değeridir. Her KKS için bu değerler Çizelge 2.1'deki maksimum sapma miktarları olacak şekilde belirlenmiştir.

$$H = [I_{3x3}\ 0_{3x3}] \tag{2.6}$$

$$R_n = (\sigma_{n,maks})^2 * I_{3x3} \tag{2.7}$$

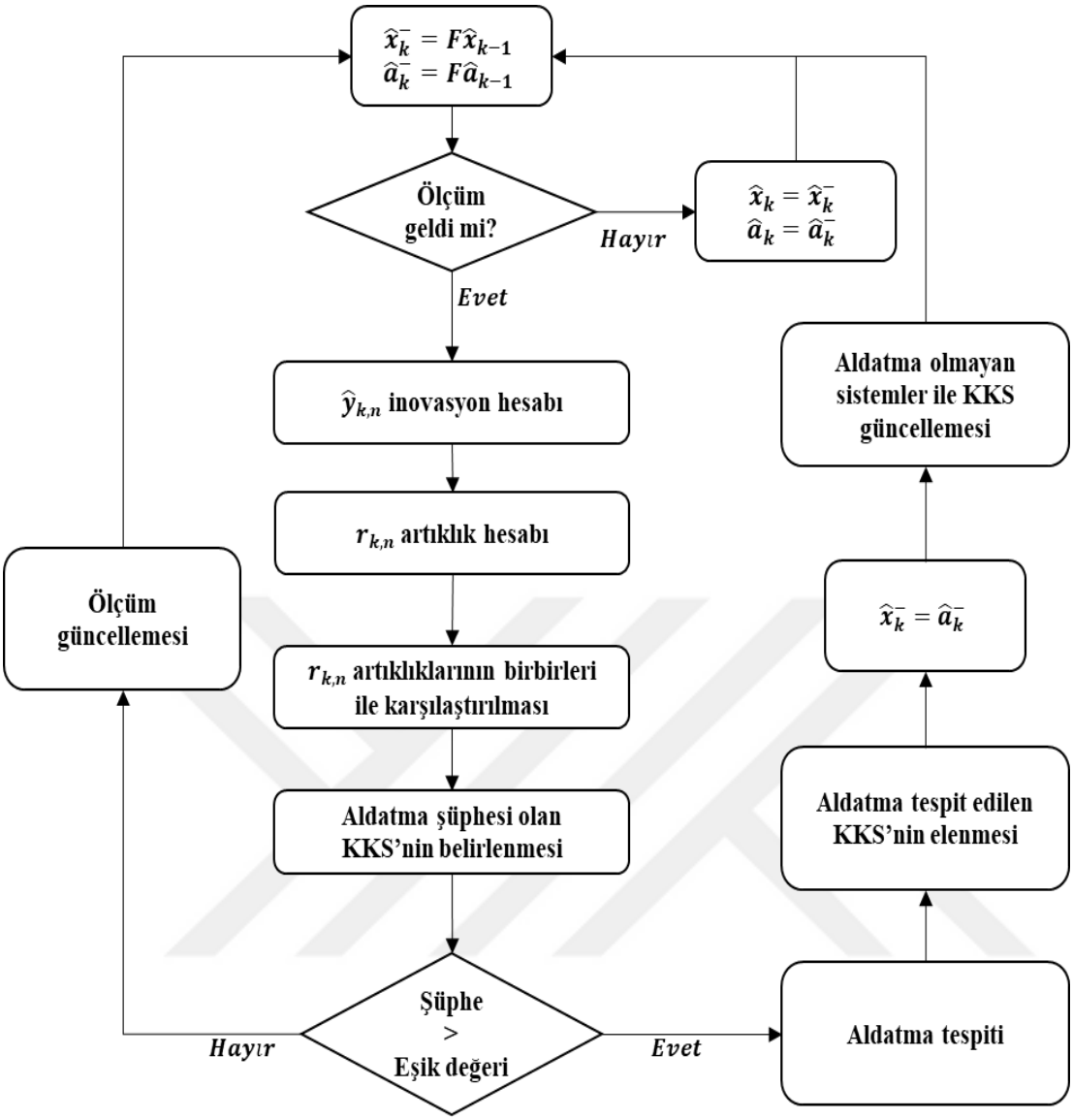
Algoritmanın Uygulanması

4 farklı küresel konumlama sisteminin sırasıyla her biri ile aldatma senaryoları oluşturulmuştur. Algoritma genel olarak, aldatma tespit edilen sistem ölçümlerine güvenilmesini keserek, diğer sistemlerden gelen ölçümler ile konumlama çözümü sunulması esasına dayanan bir Kalman filtresi yaklaşımı sunmaktadır. Önerilen Kalman filtresi tasarımı akış diyagramı Şekil 2.2'de verilmiştir [62].

Akış diyagramında da belirtildiği üzere, algoritma, durum tahminlerinin hesaplanması ile başlamaktadır. Filtrenin durum tahminleri Eşitlik (2.8) ve Eşitlik (2.9)'daki gibi oluşturulmaktadır. Bu eşitliklerdeki $\hat{x}_k$ durum tahminleri, herhangi bir aldatma tespiti yapılmadığı sürece, $\hat{a}_k$ durum tahminleri ise herhangi bir KKS ölçümü gelmediği sürece kullanılmaktadır. Eşitliklerdeki k alt simgesi ise, zaman adımlarını temsil etmektedir.

$$\hat{x}_k = \hat{x}_k^- \tag{2.8}$$

$$\hat{a}_k = \hat{a}_k^- \tag{2.9}$$



Şekil 2.2: Kalman filtresi tasarımı akış diyagramı

Anlık durum tahminleri Eşitlik (2.10) ve Eşitlik (2.11)'de belirtildiği gibi hesaplanmaktadır.

$$\hat{x}_k^- = F\hat{x}_{k-1} \tag{2.10}$$

$$\hat{a}_k^- = F\hat{a}_{k-1} \tag{2.11}$$

Filtrenin her zaman adımında, herhangi bir KKS ölçümü gelip gelmediği kontrol edilmektedir. Tüm küresel konumlama sistemleri için saniyede 1 ölçüm geldiği varsayılmış ve Kalman filtresi frekansı 5 Hz olarak belirlenmiştir. Dolayısıyla, filtrenin her 5 iterasyonunda KKS ölçümleri gelmekte ve ölçümler filtrenin düzeltme aşamasında kullanılmaktadır.

KKS ölçümleri gelmediği sürece, ölçümler gelinceye kadar, Eşitlik (2.8) ve Eşitlik (2.9)'da verildiği gibi durum tahminleri yapılmaya devam edilmektedir.

KKS ölçümleri geldiğinde, durum tahmini Eşitlik (2.12) ve Eşitlik (2.13)'te belirtildiği gibi hesaplanmaktadır.

$$\hat{x}_k = \hat{x}_k^- + güncelleme \tag{2.12}$$

$$güncelleme = \frac{1}{4} * \sum_{n=1}^{4} (K_{k,n} * \hat{y}_{k,n}) \tag{2.13}$$

Eşitlik (2.13)'te $güncelleme$ olarak verilen ifade, durum güncellemesini tanımlamakta olup, tüm KKS'lerden gelen ölçüm güncellemelerinin ortalaması olarak hesaplanmaktadır.

Burada $\hat{y}_{k,n}$ inovasyon hesabı olup, Eşitlik (2.14)'teki gibi yapılmaktadır. $z_{k,n}$ ifadesi, n'inci KKS için gelen ölçümleri temsil etmektedir.

$$\hat{y}_{k,n} = z_{k,n} - H\hat{x}_k^- \tag{2.14}$$

Hata kovaryansı matrisi hesabı Eşitlik (2.15)'te verilmiştir. Bu eşitlikteki $\overline{K_k}$, ortalama Kalman kazancını ifade etmekte olup, tüm KKS ölçümleri ile ayrı ayrı hesaplanan Kalman kazançlarının ortalamasıdır.

$$P_k = (I - \overline{K_k} * H)P_k^- \tag{2.15}$$

Bu hesaplamalar, herhangi bir aldatma tespiti olmadığı sürece geçerli sayılmaktadır.

Artıklık Hesabı

Aldatma tespitinin yapılabilmesi için artıklık hesabı yönteminden faydalanılmıştır. Artıklık hesabı Eşitlik (2.16)'da verildiği gibi yapılmakta olup, her KKS için ayrı ayrı hesaplanarak filtreye eklenmiştir.

$$r_{k,n} = \frac{z_{k,n} - H\hat{x}_k^-}{\sqrt{\left\|z_{k,n}\right\|^2 + (z_{k,n} - H\hat{x}_k^-)^2}} \tag{2.16}$$

Aldatma Tespiti

Aldatma saldırısı tespiti yapılabilmesi için her KKS için hesaplanan artıklık değerlerinin mutlak farkları birbirleri ile karşılaştırılmaktadır. Artıklık değeri, diğer KKS artıklıklarından farklı olan sistemin, aldatma saldırısı uygulayan sistem adayı olduğu belirlenmiş olmaktadır. Önceden belirlenmiş bir eşik değeri olan 10 zaman adımı boyunca, artıklık hesabı karşılaştırılmasında, aynı sistem üzerinde anormallik tespit edilmiş ise, aldatma saldırısının tespit edildiği söylenmektedir. Eşik değeri parametresinin 10 olarak belirlenmesine ilişkin detaylar, 2.3 bölümünde anlatılmaktadır.

Filtre, aldatma saldırısı olduğunun tespitini yaptıktan sonra, o KKS'den gelen ölçümlere güvenmeyi bırakmaktadır. Durum tahmini hesabını Eşitlik (2.8)'de verildiği gibi yapmayı keserek, Eşitlik (2.9)'daki gibi hesaplamaya ve aldatma olmayan sistemlerden gelen ölçümleri kullanmaya başlamaktadır.

Herhangi bir KKS'de aldatma tespiti yapıldıktan sonra $güncelleme$ hesabı Eşitlik (2.17)'de belirtildiği gibi hesaplanmaya başlamaktadır.

$$güncelleme = \frac{1}{3} * \sum_{n=1}^{3} (K_{k,n} * \hat{y}_{k,n}),$$

$$n \neq aldatma\ tespiti\ yapılan\ KKS \tag{2.17}$$

2.3 Monte-Carlo ile Simülasyon Sonuçlarının İncelenmesi

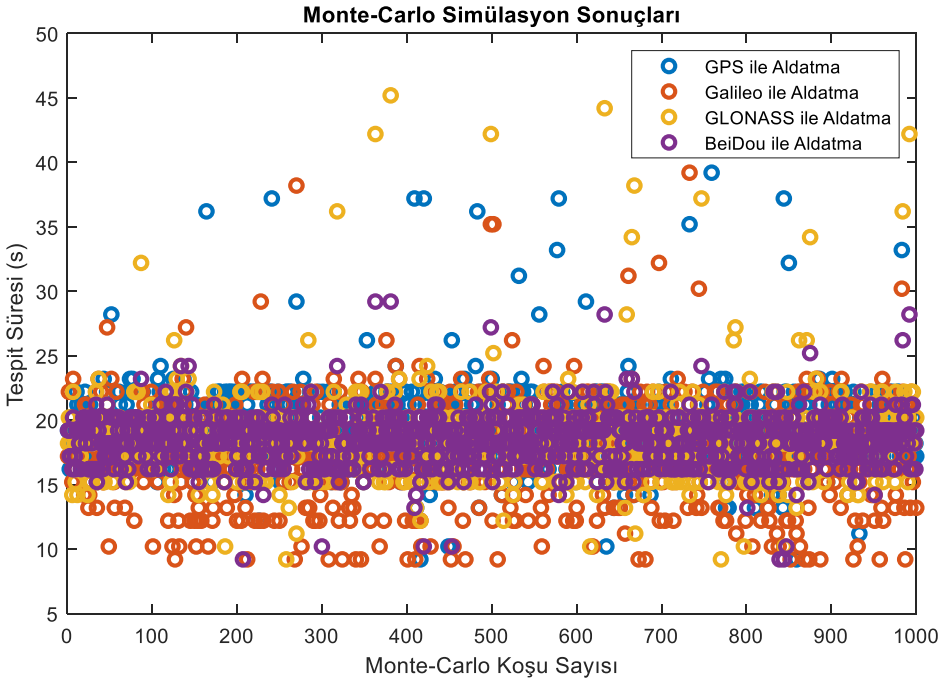
Tasarlanan Kalman filtresinin başarımını değerlendirebilmek için 1000 koşuluk bir Monte-Carlo simülasyonu oluşturulmuştur. Sırasıyla GPS, Galileo, GLONASS, BeiDou sistemleri üzerinde aldatma saldırılarının gerçekleştirildiği senaryolar incelenmiştir.

Monte-Carlo simülasyonu parametreleri KKS sistemlerinin oluşturduğu pozisyon çözümünün yatay eksendeki hata sapması değerleri olarak belirlenmiştir. Yatay eksendeki pozisyon sapmaları 1-sigma olarak belirtilen pozisyonlama doğruluklarının üzerine normal dağılım ile hata eklenmesi ile oluşturulmuştur.

Bu senaryolar altında, Monte-Carlo koşu sayılarına karşılık aldatma tespit zamanları Şekil 2.3'te verildiği gibi elde edilmiştir. Benzer şekilde, bu senaryolarda elde edilen ortalama aldatma tespit süreleri ve aldatma tespiti başarımı yüzdeleri Çizelge 2.2'de sunulduğu gibi elde edilmiştir. Sonuçlardan da görüldüğü üzere, en yüksek konumlama doğruluğuna sahip sistem olan GPS ile aldatma uygulandığı senaryoda, ortalama tespit süresi daha yüksek gözlenmiştir. Bunun sebebi, daha az güvenilir olan diğer sistemler ile bu saldırının tespit edilmeye çalışılmasıdır. Filtrenin aldatma tespit performansı ortalama aldatma süresi ve yüzde aldatma tespiti başarımı kriterleri açısından değerlendirildiğinde, aldatmanın farklı sistemler üzerinde uygulandığı 4 farklı senaryoda da benzer ve yüksek tespit performanslarında çalıştığı görülmüştür.

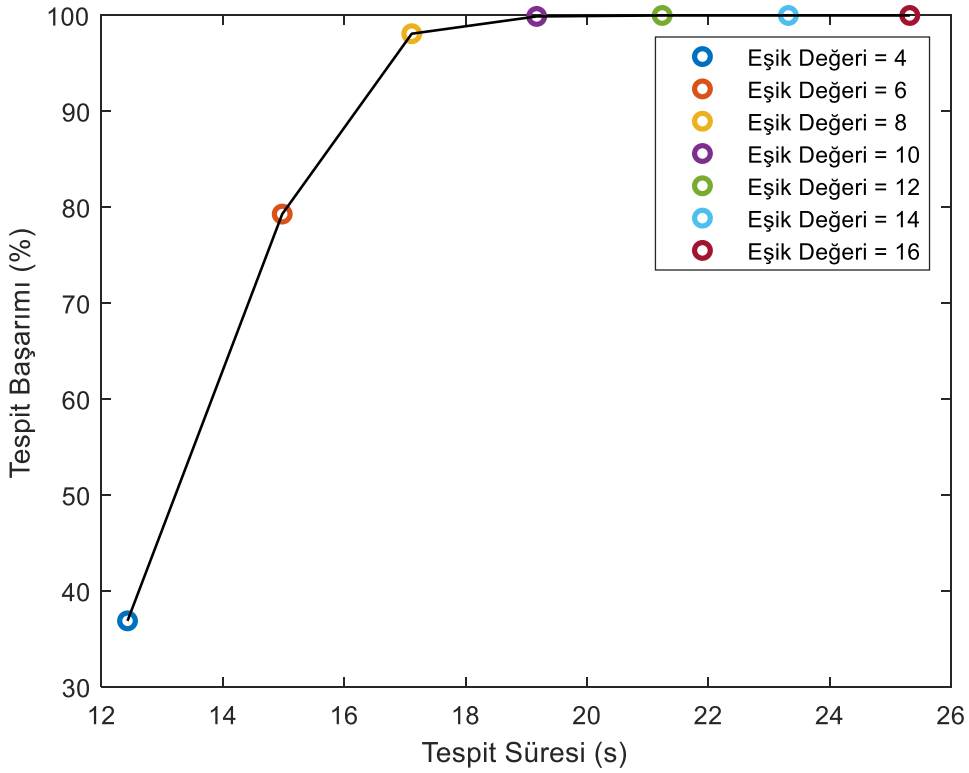
Çizelge 2.2: Aldatma saldırıları tespit performansları

Aldatma Saldırısının Uygulandığı Küresel Konumlama Sistemleri	Ortalama Aldatma Tespit Süresi (s)	Yüzde Aldatma Tespit Başarımı (%)
GPS	19.18	99.8
Galileo	17.68	97.5
GLONASS	18.72	100
BeiDou	18.47	99.9



Şekil 2.3: Aldatma tespit süreleri için Monte-Carlo simülasyon sonuçları

2.2.3 bölümünde belirtildiği üzere, aldatma tespiti yapıldığının söylenebilmesi için, herhangi bir KKS üzerinde ve belli bir eşik değeri zamanı kadar şüpheli ölçümlerin tespit edilmesi gerekmektedir. Farklı eşik değerleri için 1000 koşuluk Monte-Carlo simülasyonu yapılarak aldatma tespit başarımlarına karşılık tespit süreleri Şekil 2.4'te incelenmiştir. Tespit başarımı, aldatma uygulanan sistemin doğru olarak tespitinin yapılıp yapılamaması durumunun yüzdelik hesaplanmasıdır. Olabildiğince yüksek tespit başarımı ve düşük tespit süresinde aldatma tespitinin yapılabilmesi, buna karşılık olarak kullanılması gereken eşik değerinin belirlenmesi amaçlanmaktadır. Elde edilen grafikten de görüldüğü üzere, aldatma tespit başarımı arttıkça, tespit süresi de artmaktadır. Eşik değerinin 10 saniye olarak belirlenmesi kabul edilebilir seviyede bir tespit başarımı ve olabildiğince düşük tespit süresi elde edilmesi açısından uygun görülmüştür.



Şekil 2.4: Farklı eşik değerleri için Monte-Carlo simülasyon başarımı sonuçları

Eşik değeri 10 saniye olarak belirlendiğinde, GPS için aldatma tespit süresi yaklaşık 19 saniye olarak gözlenmiştir. Simülasyon başladığından itibaren ilk 9 saniyede boyunca, gerçek yörünge ile aldatma yörüngesi birbirlerine çok yakın olduğundan, başka bir deyişle KKS'lerin pozisyon doğrulukları seviyesi içerisinde konum sonuçları üretildiğinden, bu süre boyunca aldatma olmasından şüphelenilmemiştir. Aldatma şüphesi tespit edildikten eşik değeri süre (10 saniye) sonra aldatma var kararı alınmaktadır. Bu nedenle aldatma tespit süreleri yaklaşık 19 saniye olarak görülmüştür.

3. FARKLI KÜRESEL KONUMLAMA SİSTEMİ VE İVMEÖLÇER TÜMLEŞİMİ İLE ALDATMA SALDIRISI TESPİTİ VE ALDATMAYA KARŞI ÖNLEM İÇİN KALMAN FİLTRESİ TASARIMI

3.1 Amaç

Bu bölümde, KKS alıcısına ek olarak entegre edilen bir ivmeölçer ile aldatma tespiti algoritmasının geliştirilmesi hedeflenmektedir. 2.2.3 bölümünde önerilen yaklaşım, sadece küresel konumlama sistemleri ölçümlerini kullanarak aldatma tespiti yapmaya çalışmaktadır. Dolayısıyla, tek bir sistemden aldatma uygulandığında başarılı tespit sonuçları elde edilebilmesine rağmen, birden fazla KKS sistemi üzerinde aldatmanın uygulanabileceği senaryolar için yetersiz kalmaktadır.

Bu bölümde, 2.2.3 bölümünde önerilen yaklaşıma ek olarak ivmeölçer eklenerek ANS çözümleri Kalman filtresi ölçümlerine girdi olarak eklenmiştir. Böylelikle birden fazla KKS üzerinde aldatma saldırıları olduğunda da ivmeölçerden gelen ölçümler ile de tespit edilebilmesinin sağlanması amaçlanmıştır.

3.2 Algoritmanın Uygulanması

Bu bölümde önerilen yaklaşımın akış diyagramı, 2.2.3 bölümünde Şekil 2.2'de verilen yapıya oldukça benzer olup, ivmeölçer ölçümleri ile elde edilen ANS artıklıklarının da karşılaştırılması ile aldatma tespiti algoritması geliştirilmiştir. Böylece, birden fazla KKS ile aldatma saldırılarının olduğu senaryolara karşı tespit yeteneği kazandırılmıştır.

İvmeölçer ile ANS modellemesi ve bu sistemin KKS alıcısına entegre edilerek aldatma saldırıları tespiti amacıyla Kalman filtresinde kullanımı ilerleyen bölümlerde anlatılmaktadır.

3.2.1 İvmeölçer modellenmesi

İvmeölçer modellemesi için Inertial Sense firmasının IMX-5 modeli içerisinde kullanılan ivmeölçerden faydalanılmıştır. Bu ivmeölçer 19 µg sapma kararsızlığına ve 0.02 $\frac{m/s}{\sqrt{saat}}$ rastgele yürüyüş hata değerine sahiptir [63].

İvmeölçer ile ölçümlenen değerlerin elde edilebilmesi için Eşitlik (1.10)'da verilen ifadenin Eşitlik (3.1)'de verildiği gibi basitleştirilmiş hali kullanılmıştır. Hata kaynakları olarak en büyük etkiye sahip olacak sabit kayma (sapma) ve rastgele yürüyüş hataları eklenmiştir.

$$\begin{bmatrix} \tilde{a}_x \\ \tilde{a}_y \\ \tilde{a}_z \end{bmatrix} = \begin{bmatrix} a_x \\ a_y \\ a_z \end{bmatrix} + \begin{bmatrix} B_x \\ B_y \\ B_z \end{bmatrix} + \begin{bmatrix} \eta_x \\ \eta_y \\ \eta_z \end{bmatrix} \tag{3.1}$$

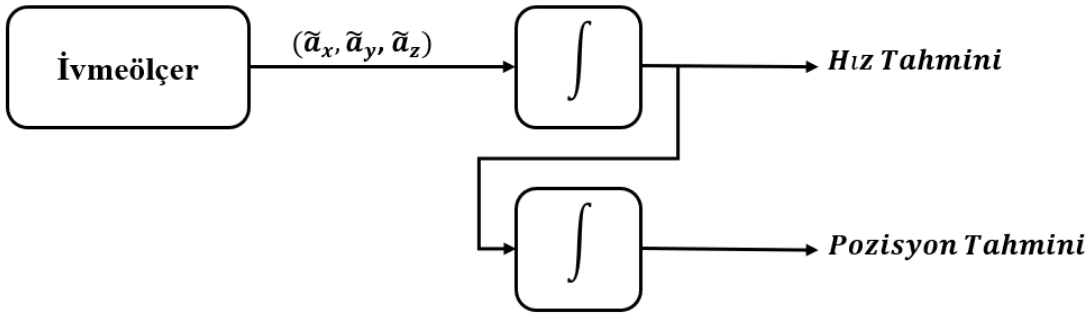
Üç eksende gerçek ivme değerlerinin hesaplanabilmesi için, gerçek hareket yörüngesinde tanımlanan gerçek pozisyon verilerinin türevi alınmıştır. Bir defa türevin alınması ile gerçek hız, ikinci defa türevin de alınması ile gerçek ivme (a_x, a_y, a_z) değerleri elde edilmiştir.

19 µg olarak belirtilen sapma kararsızlığı hatası ve 0.02 $\frac{m/s}{\sqrt{saat}}$ olarak verilen rastgele yürüyüş hatası için birim dönüşümleri sırasıyla Eşitlik (3.2) ve Eşitlik (3.3)'te verildiği gibi yapılmış, bu aralıkta rastgele hatalar olacak şekilde eklenmiştir.

$$19\mu g = 19 * g * 10^{-6}\ m/s^2 \tag{3.2}$$

$$\frac{0.02\ m/s}{\sqrt{saat}} = \frac{0.02\ m/s}{\sqrt{3600\ s}} \rightarrow \frac{0.02\ m/s}{60\sqrt{s}}\, x \frac{1}{\sqrt{dt * s}} m/s^2 \tag{3.3}$$

Gerçek ivme ve hataların eklenmesi ile üretilmiş olan ivme ölçüm değerleri ($\tilde{a}_x, \tilde{a}_y, \tilde{a}_z$), Şekil 3.1'de de görüldüğü üzere iki kez integral işlemine tâbi tutularak basit bir ANS modellemesi yapılmıştır. İlk integral işlemi ile hız tahminleri, ikinci integral işlemi ile de pozisyon tahminleri elde edilmiştir [64].

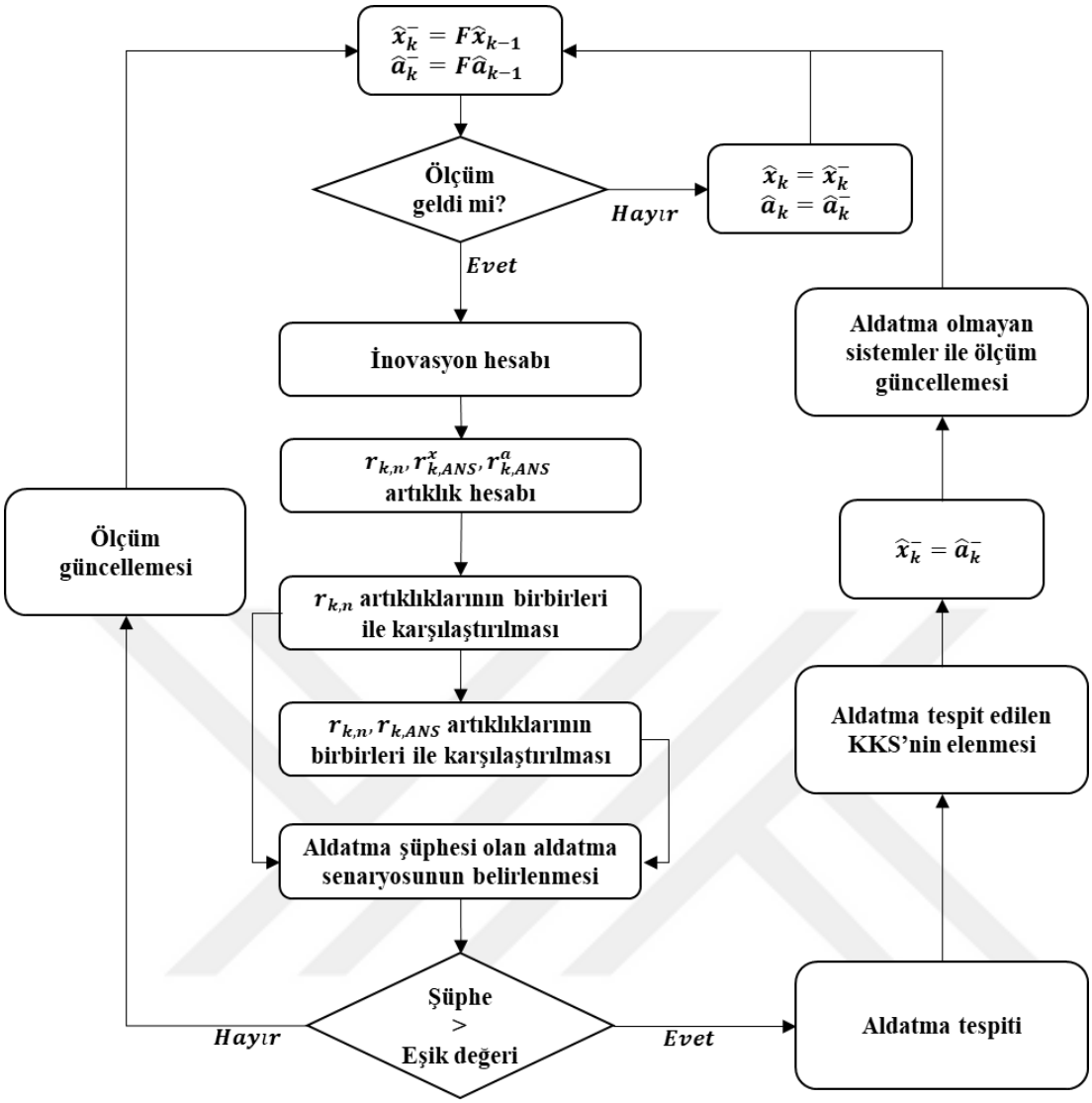


Şekil 3.1: İvmeölçer ölçümleri ile pozisyon ve hız tahmini diyagramı

3.2.2 Kalman filtresi tasarımı ve algoritmanın detayları

Genel Kalman filtresi detayları ve denklemleri, Bölüm 2.2.3'te verildiği gibi olup, güncellenen akış diyagramı Şekil 3.2'de verilmiştir.

İvmeölçerin sisteme dahil edilmesi sayesinde, ANS çözümleriyle de artıklık hesaplarının yapılarak aldatma tespiti senaryolarının genişletilmesi sağlanmış olup, algoritmanın detayları bu bölümün ilerleyen kısımlarında anlatılmaktadır.



Şekil 3.2: İvmeölçer eklenmesi ile güncellenen Kalman filtresi tasarımı akış diyagramı

Artıklık Hesabı

Küresel konumlama sistemleri ölçümleri ile ayrı ayrı artıklık hesabı, 2.3. bölümde anlatıldığı gibi, bu bölümde de yapılmaktadır. Bu bölümde ek olarak, ivmeölçer ölçümlerinden elde edilen ANS çözümleri için de artıklık hesabı yapılmaktadır.

ANS çözümleri ile artıklık hesabı, $\hat{x}_k^-$ ve $\hat{a}_k^-$ durum tahminlerinin ikisi için de ayrı ayrı olarak, Eşitlik (3.4) ve Eşitlik (3.5)'te belirtildiği gibi hesaplanmaktadır.

$$r_{k,ANS}^{x} = \frac{z_{k,ANS} - H\hat{x}_k^-}{\sqrt{\left\|z_{k,ANS}\right\|^2 + (z_{k,ANS} - H\hat{x}_k^-)^2}} \tag{3.4}$$

$$r_{k,ANS}^{a} = \frac{z_{k,ANS} - H\hat{a}_k^-}{\sqrt{\left\|z_{k,ANS}\right\|^2 + (z_{k,ANS} - H\hat{a}_k^-)^2}} \tag{3.5}$$

$\hat{x}_k^-$ durumları aldatma tespiti yapılmadığı sürece kullanılmakta olup, $\hat{a}_k^-$ durumu ile artıklık hesabının yapılmasının da eklenmesiyle hiçbir KKS'den aldatma uygulanmıyor olması ve tüm KKS'lerden aldatma uygulanıyor olması durumlarının ayırt edilebilmesi için eklenmiştir.

Aldatma Tespiti

KKS alıcısı içerisinde tasarlanan bu Kalman filtresi, ortamda aldatma sinyalleri olup olmadığını, varsa da hangi sistemler üzerinde aldatmanın uygulandığını bilmemektedir. Dolayısıyla, olası tüm aldatma kombinasyonu senaryolarında çalışacak bir algoritma kurulması ihtiyacı ortaya çıkmıştır.

İvmeölçerin de sisteme eklenmesi ile, farklı küresel konumlama sistemleri üzerinde aldatma uygulandığı senaryolarının incelenebilmesi olanağı sağlanmıştır. Alıcıda, 4 farklı KKS ile konumlama çözümü üretildiği varsayıldığından, $2^4 = 16$ farklı senaryo oluşmaktadır. Oluşan bu olası aldatma senaryoları kombinasyonları Çizelge 3.1'de verildiği gibidir.

Burada (0) ile numaralandırılan KKS'ler ile aldatma saldırısı uygulanmadığı, (1) ile numaralandırılan KKS'ler ile aldatma saldırısının uygulandığı ifade edilmektedir.

Çizelge 3.1: Olası aldatma saldırısı senaryoları kombinasyonları

Senaryo Kombinasyonları	GPS	GALILEO	GLONASS	BEIDOU
(0000)	-	-	-	-
(1000)	+	-	-	-
(0100)	-	+	-	-
(0010)	-	-	+	-
(0001)	-	-	-	+
(1100)	+	+	-	-
(1010)	+	-	+	-
(1001)	+	-	-	+
(0110)	-	+	+	-
(0101)	-	+	-	+
(0011)	-	-	+	+
(1110)	+	+	+	-
(1101)	+	+	-	+
(1011)	+	-	+	+
(0111)	-	+	+	+
(1111)	+	+	+	+

Hiçbir KKS üzerinde aldatma saldırısının uygulanmadığı, 1, 2 ve 3 KKS üzerinde aldatma uygulandığı, tüm KKS'ler üzerinde aldatma uygulandığı senaryolarının hepsi için geçerli olacak yeni bir aldatma tespiti yaklaşımı önerilmektedir.

Önerilen bu yeni yaklaşım; KKS artıklık hesaplarının hem kendi aralarında hem de ANS artıklık değerleri ile karşılaştırılması sonucunda aldatma tespiti yapılmasını esas almaktadır. Olası aldatma senaryolarına örnek olan durumlar için algoritmanın karar verme mekanizması Şekil 3.3, Şekil 3.5, Şekil 3.7, Şekil 3.9 ve Şekil 3.11'deki tablolar ile açıklanmıştır. (a) tablosunda KKS sistemlerinin artıklık hesaplarının birbirleri ile arasındaki farklar karşılaştırılarak düşük ya da yüksek olması durumları incelenmektedir. Burada, KKS artıklıkları arasındaki fark 40 kattan büyük ise yüksek olarak kabul edilmektedir. (b) tablosunda ise KKS sistemleri artıklıkları ile ANS ölçümlerinden gelen ANS çözümlerinin artıklıkları arasındaki mutlak farklar incelenmektedir. ANS çözümleri artıklıkları ile arasındaki mutlak farkın daha büyük olduğu KKS'ye büyüktür işareti (>), daha küçük olduğu KKS'ye küçüktür işareti (<),

yorum yapılamaz olan durumlara da soru işareti (?) konulmaktadır. Burada ise, artıklık ilişkileri 2 katından büyük ise büyük (>) olarak kabul edilmektedir.

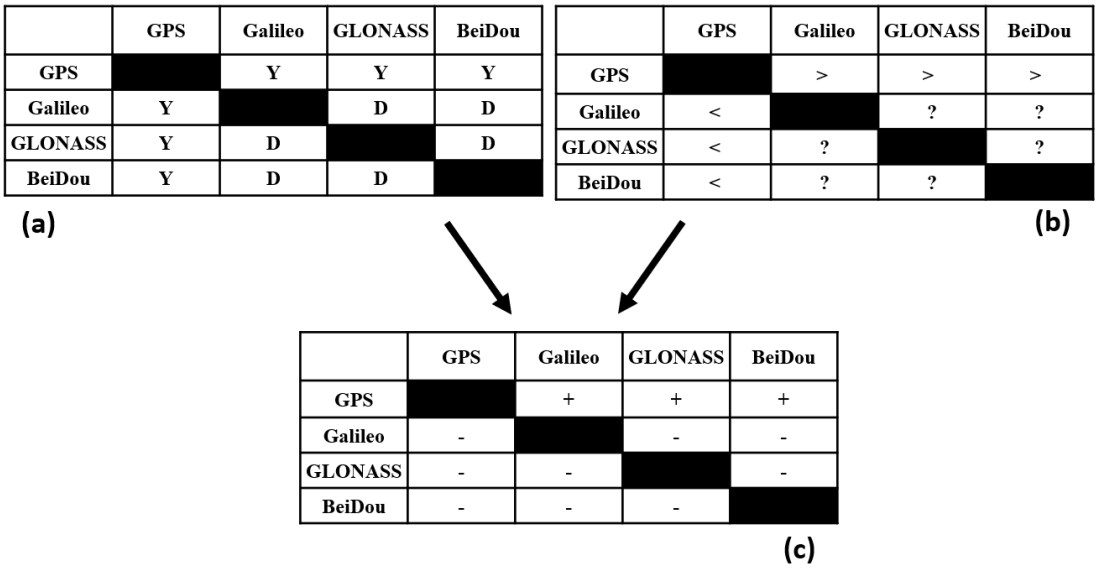
(a) ve (b) tablosunda elde edilen sonuçların bir arada değerlendirilmesi ile, hangi sistem üzerinde aldatmanın olup olmadığının tespiti de (c) tablosunda elde edilen sonuçlar ile belirlenmektedir. (a) tablosunda yüksek (Y), (b) tablosunda büyük (>) olarak belirlenen matris elemanlarına; (c) tablosunda (+), diğer tüm durumlara (-) işareti konularak aldatma şüphesi olan KKS'nin belirlenebilmesi sağlanmaktadır. (c) tablosu satırları incelenerek, (+) işareti olan satıra ait KKS üzerinde aldatma uygulandığı şüphesi olduğu kaydedilmektedir. Belli bir eşik değeri (35 saniye) zaman boyunca art arda aldatma şüphesi taşıyan bir aldatma saldırısı kombinasyonu yakalandığında, belirlenen o kombinasyondaki sistem/sistemler üzerinde aldatma uygulanıyor olduğu tespiti yapılmaktadır. Ardından, Kalman filtresinin bu KKS ölçümlerini hesaba katmadan durum tahmini yaparak devam etmesi sağlanmaktadır.

Tüm zaman adımları boyunca herhangi bir aldatma saldırısı kombinasyonu için aldatma tespiti yapılamamışsa, hiçbir KKS üzerinde aldatma saldırısının uygulanmadığı söylenmektedir.

Çizelge 3.1'de de verildiği gibi, olası tüm aldatma kombinasyonları; 1, 2 veya 3 KKS üzerinde aldatma uygulandığı, hiçbir KKS üzerinde aldatma saldırısının uygulanmadığı ve tüm KKS'ler üzerinde aldatma uygulandığı senaryolar şeklinde 5 alt başlıkta incelenebilmektedir. Önerilen aldatma tespiti algoritmasının, bu alt başlıkların hepsi için çalışmakta olduğu aşağıdaki örnekler ile anlatılmıştır.

1 KKS Üzerinde Aldatma Saldırısı Uygulanması Senaryosu

Aldatma saldırıları tek bir KKS üzerinde uygulanmakta olabilmektedir. Aldatmanın sadece GPS, sadece Galileo, sadece GLONASS ve sadece BeiDou üzerinden uygulanması senaryoları olmak üzere 4 farklı senaryo oluşmaktadır. Hepsi için aldatma kararının verilmesi durumları benzer olarak incelenmekte olup, sadece GPS üzerinde aldatma uygulanmakta olduğu bir senaryoda aldatma tespit kararının verilmesi tabloları Şekil 3.3'te verilmiştir.



	GPS	Galileo	GLONASS	BeiDou
GPS		Y	Y	Y
Galileo	Y		D	D
GLONASS	Y	D		D
BeiDou	Y	D	D	

	GPS	Galileo	GLONASS	BeiDou
GPS		>	>	>
Galileo	<		?	?
GLONASS	<	?		?
BeiDou	<	?	?	

	GPS	Galileo	GLONASS	BeiDou
GPS		+	+	+
Galileo	-		-	-
GLONASS	-	-		-
BeiDou	-	-	-	

Şekil 3.3: Sadece GPS üzerinde aldatma saldırısı uygulanması senaryosu için aldatma tespiti karar tabloları

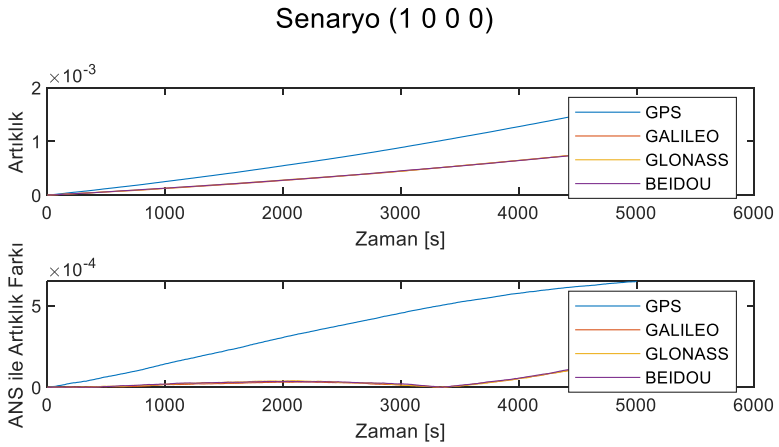
(a) tablosunda KKS'lerin artıklık değerlerinin birbirleri ile göreli büyüklükleri karşılaştırılmakta, (b) tablosunda ise KKS ile ANS çözümü artıklıkları mutlak farklarının büyüklük mertebeleri incelenmektedir.

(a) tablosunda da görüldüğü gibi, sadece GPS üzerinde aldatma saldırısının uygulandığı senaryoda, GPS'in artıklık hesabı diğer KKS'lerin artıklıkları ile karşılaştırıldığında aralarındaki mutlak fark yüksek olacaktır. Aldatmanın uygulanmadığı diğer sistemler kendi aralarında karşılaştırıldığında ise aralarındaki farkın düşük olacağı görülmektedir.

Aldatma uygulanan sistemden alınan KKS artıklıkları ile ANS artıklıkları arasında yüksek mertebelerde farklar oluşacağı, aldatma uygulanmayan KKS'ler ile ANS artıklıkları arasında düşük mertebelerde farklar oluşacağı söylenmektedir. Bu nedenle, (b) tablosunun ilk satırında, GPS ile diğer KKS'ler karşılaştırıldığında, GPS'in ANS artıklıkları arasındaki mutlak fark diğer sistemlere göre daha büyük olacaktır. Benzer şekilde, diğer KKS'ler GPS ile karşılaştırıldığında, ANS artıklıkları arasındaki mutlak farklar düşük olacaktır. Aldatma uygulanmayan sistemlerin ANS artıklıkları ile aralarındaki mutlak farklar karşılaştırıldığında ise, hepsi için düşük mertebelerde sonuçlar elde edileceğinden (?) ile işaretlenmişlerdir.

(a) tablosunda yüksek, (b) tablosunda (>) olarak belirlenen durumlar, (c) tablosunda (+), diğer tüm durumlar (-) ile işaretlenmiştir. Sadece GPS'e karşılık gelen satırda (+) işaretlendiği görülmekte olup, GPS üzerinde aldatma şüphesi olduğu söylenmektedir.

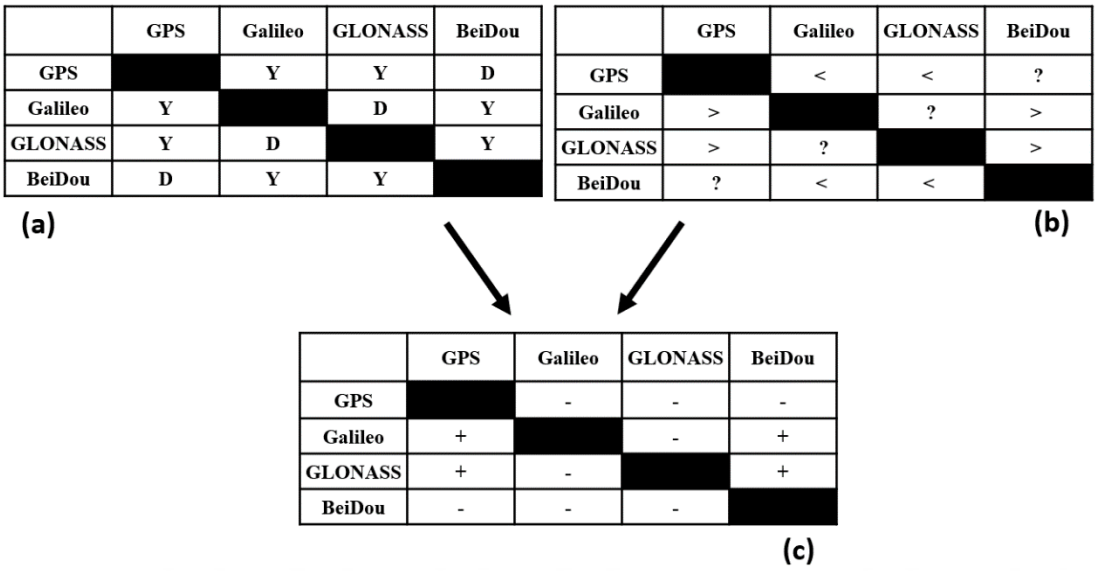
Sadece GPS ile aldatma olan bu senaryo için, KKS'ler arasındaki artıklık değerlerinin karşılaştırılması Şekil 3.4'te ilk grafikte verilmiştir. GPS için artıklık değerinin, diğer sistemlere göre oldukça yüksek olduğu görülmektedir. KKS'ler ile ANS artıklıklarının mutlak farkları Şekil 3.4'ün ikinci grafiğinde çizdirilmiştir. Aldatma uygulanmayan sistemler için bu artıklık farklarının birbirleri ile çok yakın ve aldatma uygulanan sistem için artıklık farkından oldukça düşük seviyelerde oldukları görülmektedir.



Şekil 3.4: Sadece GPS üzerinde aldatma saldırısı uygulanması senaryosu için artıklık karşılaştırma grafikleri

2 Farklı KKS Üzerinde Aldatma Saldırısı Uygulanması Senaryosu

Aldatma saldırıları iki farklı KKS üzerinde de uygulanmakta olabilmektedir. Aldatmanın iki farklı KKS üzerinde uygulanıyor olduğu 6 farklı senaryo ihtimali vardır. Hepsi için aldatma kararının verilmesi durumları benzer olarak incelenmekte olup, Galileo ve GLONASS için aldatma uygulanmakta olduğu bir senaryoda aldatma tespit kararının verilmesi tabloları Şekil 3.5'te verilmiştir.



Şekil 3.5: Galileo ve GLONASS üzerinde aldatma saldırısı uygulanması senaryosu için aldatma tespiti karar tabloları

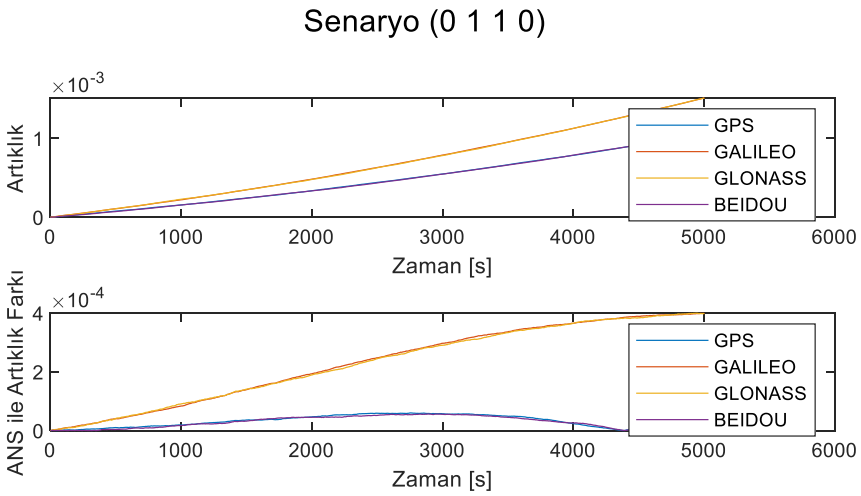
Galileo ve GLONASS üzerinde aldatma saldırısının uygulandığı senaryoda, (a) tablosunda da görüldüğü üzere, aldatmanın uygulandığı KKS'lerin artıklık hesapları aldatmanın uygulanmadığı KKS'ler ile karşılaştırılması sonuçları yüksek, aldatma uygulanan iki KKS'nin birbirleri arasında karşılaştırılması veya aldatma uygulanmayan diğer iki KKS'nin birbirleri arasında karşılaştırılması sonuçları düşük çıkmaktadır.

(b) tablosunda da görüldüğü gibi, aldatma uygulanan sistemlerin artıklık değerlerinin ANS artıklık hesapları ile mutlak farkları, uygulanmayan sistemlerin ANS artıklıkları ile mutlak farkları karşılaştırıldığında büyük olacaktır. Benzer şekilde, aldatma uygulanmayan KKS artıklıkları ile ANS artıklıklarının mutlak farkları, aldatma

uygulanan sistemlerinki ile karşılaştırıldığında daha küçük olacaktır. Aldatma uygulanmayan KKS'lerin ANS ile mutlak farklarının birbirleri ile karşılaştırılmasında ve aldatma uygulanan KKS'lerin ANS ile mutlak farklarının birbirleri ile karşılaştırılmasında yorum yapılamamaktadır.

(a) tablosunda yüksek, (b) tablosunda (>) olarak belirlenen durumlar, (c) tablosunda (+), diğer tüm durumlar (-) ile işaretlenip elde edilen tablonun satırları incelendiğinde, Galileo ve GLONASS sistemleri için (+) oluştuğu görülmüştür. Bu sebeple, Galileo ve GLONASS üzerinde aldatma saldırısı şüphesi olduğu söylenmektedir.

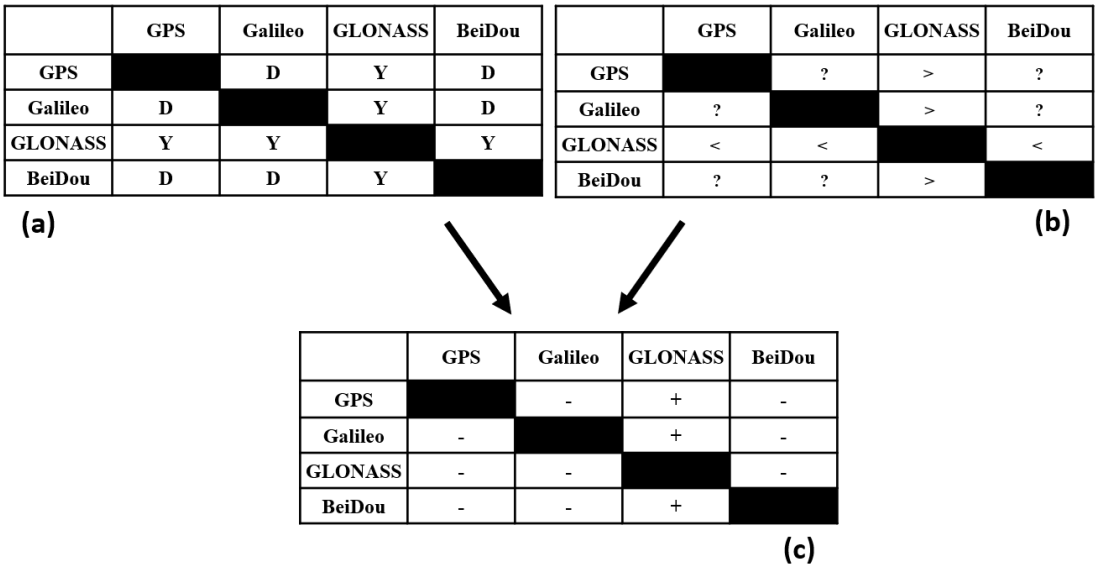
Bu senaryo için artıklık değerlerinin karşılaştırılma grafikleri Şekil 3.6'da verilmiştir. İlk grafikte görüldüğü gibi, aldatma uygulanmayan KKS'lerin artıklık değerleri birbirlerine çok yakın ve düşük mertebelerde, aldatma uygulanan sistemlerinki ise yine birbirlerine çok yakın ve daha yüksek artıklık değerleri ile elde edilmektedir. KKS'lerin ANS çözümü artıklıkları ile karşılaştırılması ise ikinci grafikte verilmiştir. Aldatma uygulanmayan sistemlerin ANS ile artıklık mutlak farkları kendi aralarında aynı seviyelerde ve daha düşük, aldatma uygulanan sistemlerinki ise daha yüksek çıkmaktadır.



Şekil 3.6: Galileo ve GLONASS üzerinde aldatma saldırısı uygulanması senaryosu için artıklık karşılaştırma grafikleri

3 Farklı KKS Üzerinde Aldatma Saldırısı Uygulanması Senaryosu

Aldatma saldırıları, aynı anda üç farklı KKS üzerinde de uygulanıyor olabilmektedir. Aldatmanın üç farklı KKS üzerinde uygulandığı 4 farklı senaryo oluşmaktadır. Hepsi için aldatma kararının verilmesi durumları benzer olarak incelenmekte olup; GPS, Galileo ve BeiDou için aldatma uygulanmakta olduğu bir senaryoda aldatma tespit kararının verilmesi tabloları Şekil 3.7'de verilmiştir.



	GPS	Galileo	GLONASS	BeiDou
GPS		D	Y	D
Galileo	D		Y	D
GLONASS	Y	Y		Y
BeiDou	D	D	Y	

	GPS	Galileo	GLONASS	BeiDou
GPS		?	>	?
Galileo	?		>	?
GLONASS	<	<		<
BeiDou	?	?	>	

	GPS	Galileo	GLONASS	BeiDou
GPS		-	+	-
Galileo	-		+	-
GLONASS	-	-		-
BeiDou	-	-	+	

Şekil 3.7: GPS, Galileo ve BeiDou üzerinde aldatma saldırısı uygulanması senaryosu için aldatma tespiti karar tabloları

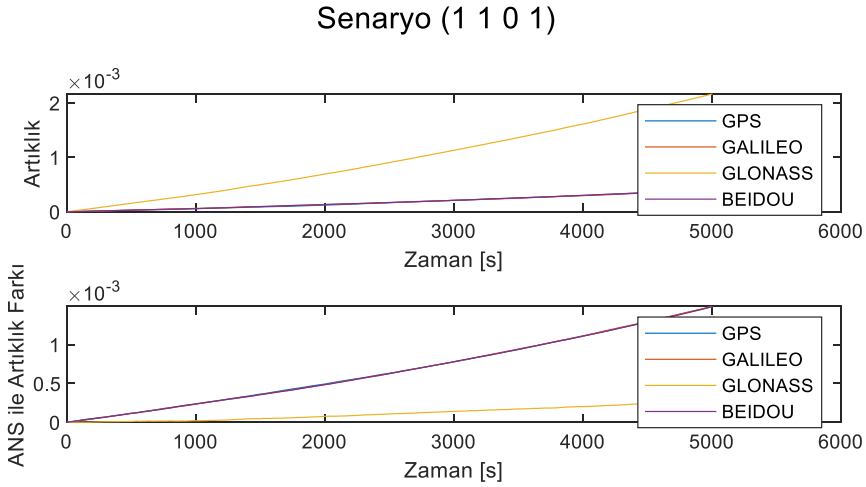
GPS, Galileo ve BeiDou üzerinde aldatma saldırısının uygulandığı senaryoda, (a) tablosunda da görüldüğü üzere, sadece GLONASS ile doğru ölçümler geliyor olduğundan, GLONASS artıklıkları diğer sistemlerin artıklıkları ile karşılaştırıldığında yüksek, diğer sistemlerin artıklıkları kendi aralarında karşılaştırıldığında daha düşük seviyelerde çıkmaktadır.

(b) tablosunda da, aldatmanın uygulanmadığı sistemin artıklığı ANS artıklıkları ile karşılaştırıldığında, aldatma uygulanan sistemlerinkinden daha düşük olacağı söylenmektedir. Bunun sebebi ANS çözümleri ile aldatma uygulanmayan sistemin artıklıklarının birbirlerine oldukça yakın olacak olmasıdır. Aldatma uygulanan sistemlerin artıklıklarının ANS artıklığı ile farkının aldatma uygulanmayan sistem ile karşılaştırılmasında ise daha büyük çıkacağı söylenmektedir. Aldatma saldırısı

uygulanan KKS ile ANS artıklıklarının mutlak farklarının birbirleri ile karşılaştırılmasında yorum yapılamamakta olup (?) ile işaretlenmektedir.

(a) tablosunda yüksek, (b) tablosunda (>) olarak bulunan koşullarda, (c) tablosunda (+), diğer tüm koşullarda (-) ile işaretlenmiştir. Oluşan tablonun satırları incelendiğinde, GPS, Galileo ve BeiDou sistemleri için (+) oluştuğu görülmüştür. Bu sebeple, GPS, Galileo ve BeiDou üzerinde aldatma saldırısı şüphesi olduğu söylenmektedir.

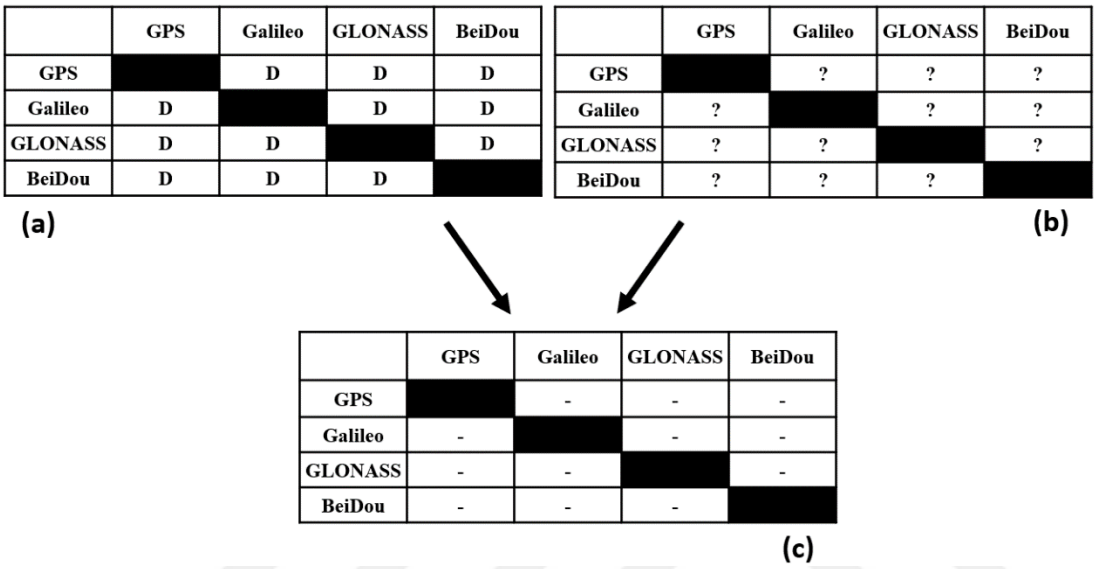
Bu senaryo için çizdirilen Şekil 3.8'in ilk grafiğinde görüldüğü gibi, aldatma uygulanan KKS'lerin artıklık değerleri birbirlerine çok yakın ve düşük seviyelerde iken, aldatma uygulanmayan sistemin artıklık değeri daha yüksek seviyede olmaktadır. İkinci grafikte de elde edildiği üzere, aldatma uygulanan KKS'lerin ANS ile mutlak artıklık farkları birbirlerine çok yakın ve yüksek seviyede, aldatma uygulanmayan sistem ile ANS artıklık değeriyle mutlak farkı ise daha düşük seviyede çıkmaktadır.



Şekil 3.8: GPS, Galileo ve BeiDou üzerinde aldatma saldırısı uygulanması senaryosu için artıklık karşılaştırma grafikleri

Hiçbir KKS Üzerinde Aldatma Saldırısı Uygulanmaması Senaryosu

Hiçbir KKS üzerinde aldatma saldırısının olmadığı, tüm sistemlerden gerçek pozisyon çözümleri elde edilebildiğinde oluşan senaryo için, aldatma tespiti kararının belirlenebilmesi için üretilen tablolar Şekil 3.9'da verilmiştir.



	GPS	Galileo	GLONASS	BeiDou
GPS		D	D	D
Galileo	D		D	D
GLONASS	D	D		D
BeiDou	D	D	D	

(a)

	GPS	Galileo	GLONASS	BeiDou
GPS		?	?	?
Galileo	?		?	?
GLONASS	?	?		?
BeiDou	?	?	?	

(b)

	GPS	Galileo	GLONASS	BeiDou
GPS		-	-	-
Galileo	-		-	-
GLONASS	-	-		-
BeiDou	-	-	-	

(c)

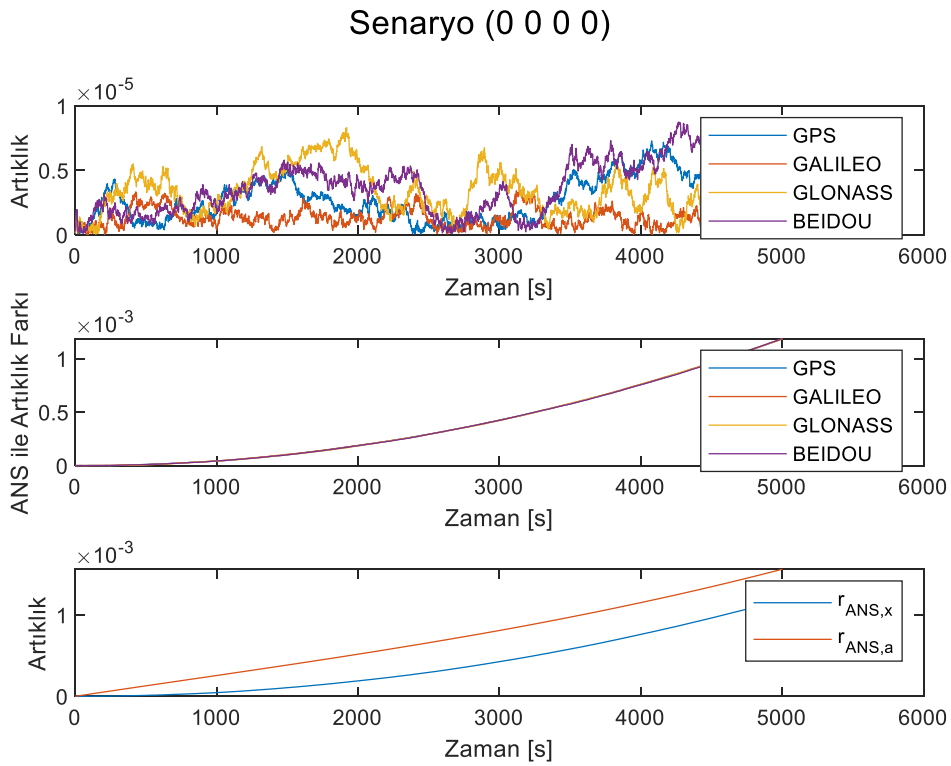
Şekil 3.9: Hiçbir KKS üzerinde aldatma saldırısı uygulanmaması senaryosu için aldatma tespiti karar tabloları

Hiçbir KKS üzerinde aldatma saldırısının uygulanmadığı senaryoda, KKS ölçümleri gerçek pozisyon değerlerine çok yakındır. Dolayısıyla hesaplanan artıklık değerleri birbirlerine oldukça yakın olmaktadır. (a) tablosunda KKS artıklık hesapları birbirleri ile karşılaştırıldığında, hepsi için aralarındaki artıklık farklarının düşük olacağı söylenebilmektedir.

(b) tablosunda, KKS ölçümlerinin ANS ölçümleri artıklıklarının mutlak farkları incelenmekte olup, tüm sistemlerden gerçeğe çok yakın ölçümler gelmekte olduğundan artıklık hesapları birbirlerine ve sıfıra çok yakın mertebelerde olmaktadır. Bu nedenle, KKS'lerin ANS çözümleri ile karşılaştırıldıklarında artıklık hesaplarının büyüklükleri hakkında yorum yapılamıyor olup, tabloda (?) ile belirtilmişlerdir.

Sonuç olarak (a) ve (b) tabloları incelenerek elde edilen (c) tablosunda, herhangi bir aldatma tespiti yapılamadığı söylenmektedir.

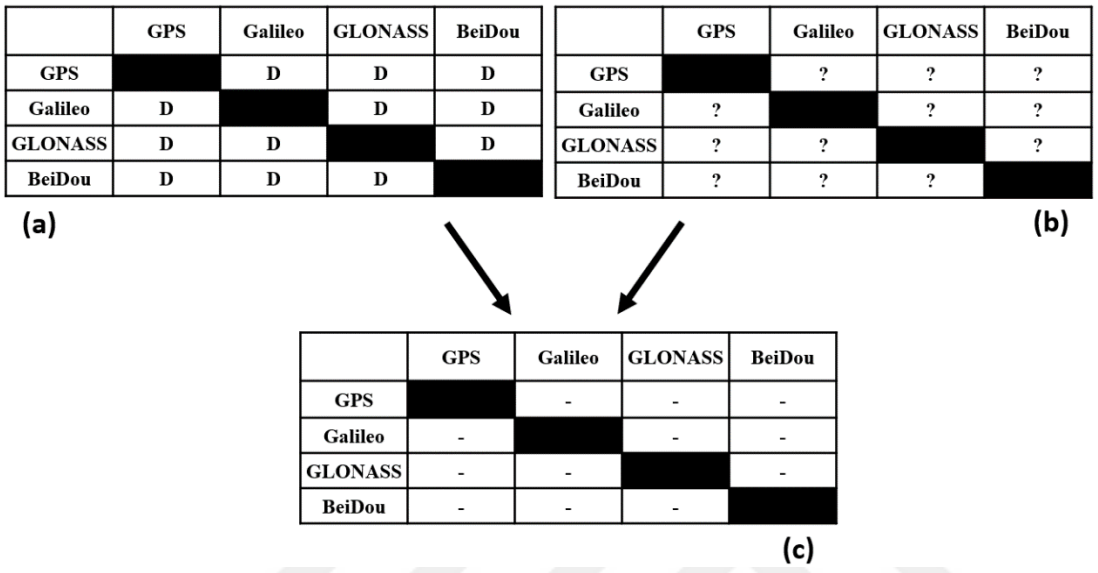
Şekil 3.10'da ilk grafikte KKS artıklık değerleri çizdirilmiş olup, hepsi sıfıra çok yakın ve benzer seviyelerdedir. İkinci grafikte de KKS artıklıkları ile ANS artıklıklarının mutlak farkları çizdirilmiş, hepsi birbirlerine çok yakın olarak elde edilmiştir. Son grafikte ise, $\hat{x}_k$ ve $\hat{a}_k$ durum tahminleri ile hesaplanan ANS artıklık değerleri çizdirilmiş olup, $\hat{x}_k$ durum tahmini ile hesaplanan artıklıkların her zaman adımında daha yüksek seviyelerde olduğu görülmüştür. $\hat{x}_k$ ve $\hat{a}_k$ durum tahminleri ile hesaplanan ANS artıklıkları, hiçbir KKS ile aldatma olmaması ve tüm KKS ile aldatma olması senaryolarının ayırt edilebilmesi için kullanılmaktadır.



Şekil 3.10: Hiçbir KKS üzerinde aldatma saldırısı uygulanmaması senaryosu için artıklık karşılaştırma grafikleri

Tüm KKS'ler Üzerinde Aldatma Saldırısı Uygulanması Senaryosu

Tüm KKS'ler üzerinde aldatma saldırısının uygulandığı senaryo için, aldatma tespiti kararının belirlenebilmesi için üretilen tablolar Şekil 3.11'de verilmiştir.



Şekil 3.11: Tüm KKS'ler üzerinde aldatma saldırısı uygulanması senaryosu için aldatma tespiti karar tabloları

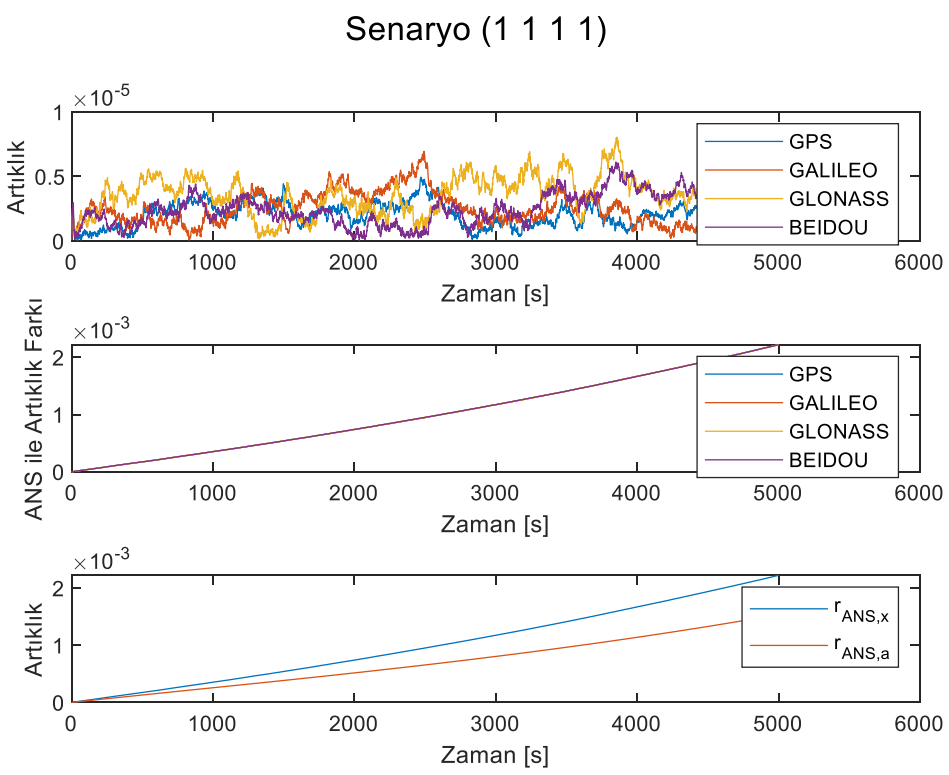
Tüm KKS'ler üzerinde aldatma saldırısının uygulandığı senaryoda, KKS ölçümleri birbirlerine oldukça yakın, ancak bu değerler gerçek pozisyon değerlerinden oldukça farklı olacaktır. Bu nedenle, (a) tablosunda belirtilen KKS artıklık hesaplarının birbirleri arasındaki farklar, tüm karşılaştırma sonuçlarında oldukça düşük olacaktır.

Benzer şekilde, KKS ile ANS çözümlerinin artıklık hesapları arasındaki mutlak farklar (b) tablosunda incelenmektedir. Tüm KKS'ler üzerinde aldatma olduğunda, bu değerler birbirlerine çok yakın çıkacak ve artıklık hesaplarının büyüklükleri hakkında yorum yapılamıyor olacaktır. Dolayısıyla, (c) tablosunda herhangi bir aldatma tespiti kararı verilemediği söylenmektedir.

Şekil 3.9 ve Şekil 3.11'de görüldüğü gibi, hiçbir KKS ile aldatma olmadığı senaryo ile tüm KKS'ler ile aldatma uygulandığında benzer tablolar elde edilmektedir. Bu senaryolardan hangisinin gerçekleşmekte olduğunun kararının verilebilmesi için $\hat{x}_k$ ve $\hat{a}_k$ durum tahminlerinden faydalanılmaktadır.

Şekil 3.10 ve Şekil 3.12'de görüldüğü gibi, tüm KKS'ler üzerinde aldatma uygulanıyor olduğu senaryoda, $\hat{a}_k$ durum tahmini ile hesaplanan ANS artıklık hesapları $\hat{x}_k$ durum tahmini ile hesaplanan artıklıklardan her zaman adımı için daha küçük çıkmaktadır. Hiçbir KKS ile aldatma uygulanmıyor olduğu senaryoda ise her zaman adımında daha büyük olarak gözlenmiştir.

Sonuç olarak; 1, 2 ya da 3 KKS üzerinde aldatma saldırısı uygulandığı kararı verilemediğinde tüm KKS'ler üzerinden aldatmanın uygulandığı ya da hiçbir KKS üzerinde aldatma uygulanmadığı senaryolardan biri gerçekleşmektedir. Olası bu iki senaryodan hangisinin uygulanmakta olduğunun kararının verilebilmesi için, algoritma $\hat{x}_k$ ve $\hat{a}_k$ durum tahminleri ile yapılan ANS artıklıklarını birbirleri ile karşılaştırmaktadır.



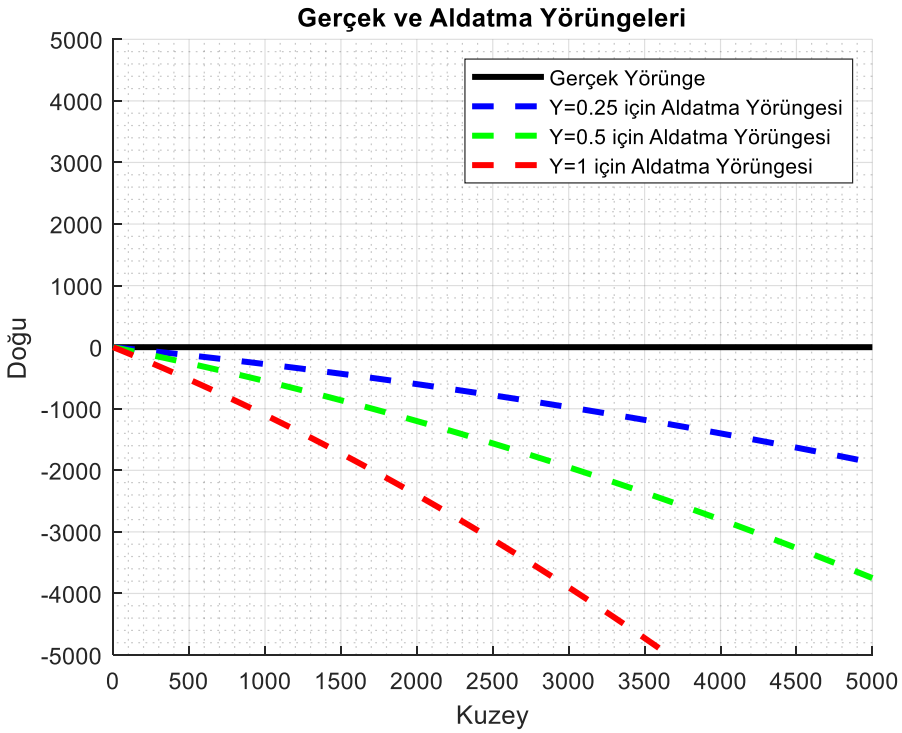
Şekil 3.12: Tüm KKS'ler üzerinde aldatma saldırısı uygulanması senaryosu için artıklık karşılaştırma grafikleri

3.3 Monte-Carlo Simülasyon Sonuçlarının İncelenmesi

Bu bölümde, farklı aldatma yörüngeleri için küresel konumlama sistemlerine uygulanan aldatma saldırılarına karşı aldatma tespit performansları incelenmektedir.

1000 koşuluk Monte-Carlo simülasyonları yapılmış olup, 3 farklı aldatma yörüngesi için başarımları değerlendirilmiştir. Oluşturulan aldatma yörüngeleri, Eşitlik (3.6)'da verildiği gibi tanımlanmış olup, bunlara karşılık gelen yörüngeler Şekil 3.13'te gösterilmiştir.

$$y_{NED} = -(x_{NED} + (0.0005 * x_{NED}).* dt) * Y, \qquad (3.6)$$
$$Y = \{0.25, 0.5, 1\}$$



Şekil 3.13: Gerçek ve aldatma yörüngeleri

Şekil 3.13'te oluşturulan aldatma yörüngeleri ile uygulanan aldatma saldırıları senaryoları için yüzde aldatma tespit performansları ve tespit süreleri 1000 koşuluk Monte-Carlo simülasyonlarında Çizelge 3.2'deki gibi elde edilmiştir. Çizelgede de görüldüğü üzere, senaryoların tümü için aldatma yörüngeleri daraldıkça genel olarak tespit başarımının azaldığı tespit süresinin de arttığı gözlenmiştir.

Çizelge 3.2: Farklı aldatma yörüngeleri için aldatma tespit performansları

	Y=1 Yörüngesi		**Y=0.5 Yörüngesi**		**Y=0.25 Yörüngesi**	
Senaryo	**Tespit Başarımı (%)**	**Tespit Süresi (s)**	**Tespit Başarımı (%)**	**Tespit Süresi (s)**	**Tespit Başarımı (%)**	**Tespit Süresi (s)**
(0000)	95,8	-	95,8	-	95,8	-
(1000)	99,6	210,396	96,8	382,732	75	655,96
(0100)	99,6	122,702	99,6	208,116	95,8	357,902
(0010)	100	75,394	100	91,656	100	135,624
(0001)	99,8	123,626	99,4	214,004	95,6	372,866
(1100)	99,6	149,906	99,6	261,196	99,4	470,162
(1010)	99,8	272,682	91,8	496,538	65,2	749,602
(1001)	99,8	150,176	99,8	263,078	99,4	441,514
(0110)	100	144,996	99,6	255,862	89,4	467,05
(0101)	99,8	275,152	98,6	484,186	81,6	787,522
(0011)	99,8	141,23	99,2	254,436	90	462,606
(1110)	100	103,858	100	182,528	99,8	325,038
(1101)	100	50,942	100	65,148	100	105,124
(1011)	100	100,216	100	176,258	99,8	313,078
(0111)	100	173,566	99,4	319,286	87,2	613,45
(1111)	100	48,168	41,8	1747,276	0	0

Tek bir KKS üzerinde aldatma saldırısı uygulanan senaryolar arasından, pozisyon doğruluğu en zayıf olan GLONASS sistemi üzerinde aldatmanın uygulandığı senaryoda, filtrenin tespit başarımı en yüksek ve %100 olarak gözlenmiştir. Bunun sebebi diğer sistemlerin daha doğru pozisyonlama sonuçları vermesi sayesinde filtrenin daha doğru tahminler yapabilmesidir.

2 KKS üzerinde aldatma saldırısının uygulandığı senaryolar arasından (1010) ve (0101) senaryolarında, algoritmanın tespit süresinin daha uzun olduğu ve diğer senaryoların kendi aralarında benzer sonuçlar verdiği gözlenmiştir.

3 KKS üzerinde birden aldatma saldırılarının uygulandığı senaryolar incelendiğinde, GLONASS hariç sistemler üzerinde aldatma uygulandığında %100 başarım ile oldukça düşük tespit sürelerinde aldatmanın tespit edilebildiği görülmüştür.

Yukarıda açıklanan gözlemlerin nedenini açıklayabilmek için filtrede ölçüm olarak kullanılan KKS verilerin baskınlık dereceleri aşağıdaki gibi incelenmiştir:

Tek bir KKS üzerinde aldatma saldırısı uygulanan senaryolarda, aldatmanın olduğu KKS ölçümünün ağırlığı diğer KKS'lere oranla düşük olacağı için bu senaryolarda aldatma uygulanmayan KKS ölçümleri filtrede baskın, aldatma uygulanan KKS ölçümleri ise resesif olacaktır.

Öte yandan, 3 KKS üzerinde aldatma saldırılarının uygulandığı senaryolarda, aldatman uygulanan KKS ölçümlerinin baskın, aldatma uygulanmayan ölçümlerin ise resesif olacağı söylenmektedir.

Ancak, 2 KKS üzerinde aldatmanın uygulandığı senaryolarda, aldatma uygulanan ve uygulanmayan KKS sayıları eşit olduğu için, baskınlık değerlendirilmesi aldatma uygulanan ve uygulanmayan KKS'lerin doğruluk değerlerine bakılarak yapılmıştır.

Yapılan baskınlık değerlendirmelerinin sonuçları Çizelge 3.3'te verilmiştir.

Bu çizelgede $\sigma_{0,t}$ ifadesi, o senaryodaki aldatma saldırısı uygulanmayan KKS'lerin pozisyon doğruluklarının toplamıdır. $\sigma_{1,t}$ ifadesi, o senaryodaki aldatma saldırısı uygulanan KKS'lerin pozisyon doğruluklarının toplamıdır. $\sigma_{b,ort}$ o senaryodaki baskın olan KKS'lerin pozisyon doğruluklarının ortalamasıdır. $\sigma_{r,ort}$ ise o senaryodaki resesif olan KKS'lerin pozisyon doğruluklarının ortalamasıdır.

Tasarlanan Kalman filtresi, artıklık değerlerinin birbirleri arasındaki açıklık ne kadar fazla ise o kadar hızlı ve doğru tespit yapabilecek bir algoritmadır. Dolayısıyla bu açıklığın baskın olan ölçümler ile resesif olan ölçümlerin doğruluk değerlerinin arasındaki oran ile ilişkili olduğu Çizelge 3.3'te gösterilmiştir.

Çizelge 3.3: Baskınlık hesabı ilişkisi çizelgesi

Senaryo	$\boldsymbol{\sigma_{0,t}}$	$\boldsymbol{\sigma_{1,t}}$	$\boldsymbol{\sigma_{b,ort}}$	$\boldsymbol{\sigma_{r,ort}}$	$\boldsymbol{\frac{\sigma_{b,ort}}{\sigma_{r,ort}}}$
(0000)	-	-	-	-	-
(1000)	**10**	2.5	3.33	2.5	1.332
(0100)	**9.5**	3	3.16	3	1.053
(0010)	**8.5**	4	2.83	4	0.708
(0001)	**9.5**	3	3.16	3	1.053
(1100)	7	**5.5**	2.75	3.5	0.786
(1010)	**6**	6.5	3	3.25	0.923
(1001)	7	**5.5**	2.75	3.5	0.786
(0110)	**5.5**	7	2.75	3.5	0.786
(0101)	6.5	**6**	3	3.25	0.923
(0011)	**5.5**	7	2.75	3.5	0.786
(1110)	3	**9.5**	3.16	3	1.053
(1101)	4	**8.5**	2.83	4	0.708
(1011)	3	**9.5**	3.16	3	1.053
(0111)	2.5	**10**	3.33	2.5	1.332
(1111)	-	-	-	-	-

Bu metrik göz önüne alındığında, tek KKS ile aldatma uygulandığı senaryolar arasından GLONASS ile aldatma uygulandığı senaryoda, $\frac{\sigma_{b,ort}}{\sigma_{r,ort}}$ değerinin en küçük çıktığı ve bu sebeple tespit süresi en hızlı olduğu görülmektedir.

Benzer şekilde, üç KKS ile aldatmanın uygulandığı senaryolar arasından, GLONASS hariç sistemler ile aldatma uygulandığında $\frac{\sigma_{b,ort}}{\sigma_{r,ort}}$ değeri en küçük olarak hesaplanmakta ve bu sebeple tespit süresi en kısa bu senaryoda gözlenmektedir.

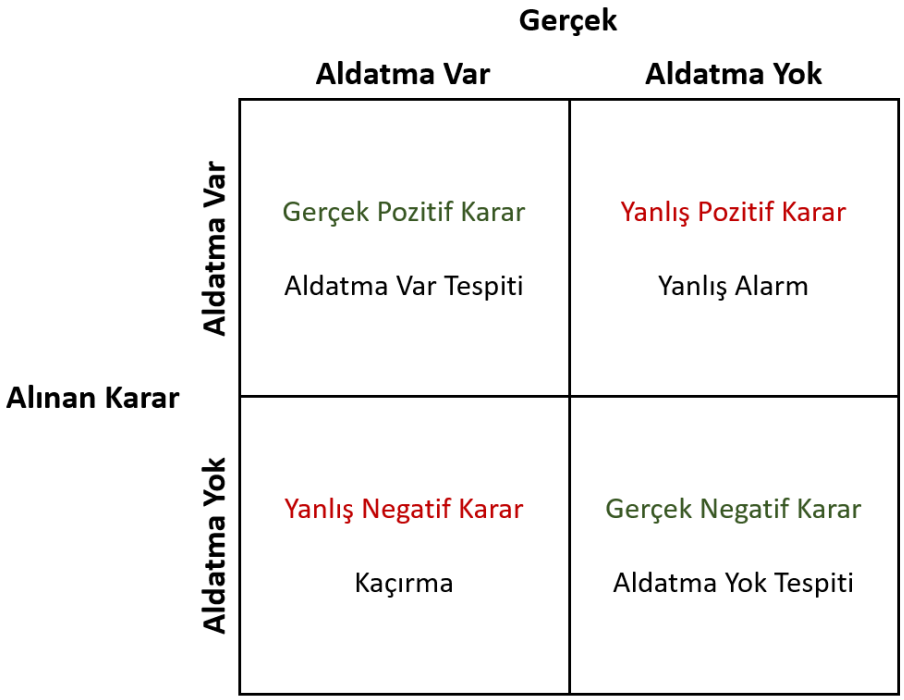
İki KKS ile aldatma uygulandığı senaryolarda ise; (1010) ve (0101) senaryolarındaki $\frac{\sigma_{b,ort}}{\sigma_{r,ort}}$ değerinin diğer senaryolardaki değerden büyük olduğu ve bu sebeple daha yüksek tespit sürelerinin olduğu görülmektedir. İki KKS ile aldatmanın olduğu diğer senaryolarda ise, $\frac{\sigma_{b,ort}}{\sigma_{r,ort}}$ değerinin aynı olarak hesaplandığı ve yakın mertebelerde tespit süresi sonuçları verdiği gözlenmiştir.

Hiçbir KKS üzerinde aldatma uygulanmadığı senaryoda, tüm aldatma yörüngeleri için %95.8 tespit başarımı sağlandığı görülmüş, tespit sürelerinden söz edilemeyeceği için (-) ile belirtilmiştir.

Tüm KKS'ler üzerinde aldatmanın uygulandığı senaryoda, Y=1 değerine sahip en geniş aldatma yörüngesi için aldatma tespit başarımı %100 ve tespit süresi yaklaşık 48 saniye ile filtrenin en hızlı tespit süresidir. En yüksek filtre performansının bu senaryoda gözlenmesinin sebebi, ANS çözümleri ile diğer tüm KKS'lerden anormal ölçümler alındığının kolaylıkla tespit edilebilmesidir. Aldatma yörüngeleri daraldıkça, KKS ölçümleri de ANS ölçümlerine yaklaştığından tespit performansları azalmaktadır. Özellikle, Y=0.25 yörüngesinde aldatma yörüngeleri ANS'nin hata biriktirerek pozisyon çözümü sunan sonuçlarına oldukça yaklaştığından aldatma tespitinin yapılamadığı görülmüştür.

ROC Eğrileri ile Filtre Başarımının İncelenmesi

Tasarlanan bir dedektörün başarımını test edebilmek için yaygın olarak kullanılan yöntemlerden biri ROC (receiver operating characteristic / alıcı çalışma karakteristiği) eğrilerinin çizdirilmesidir. ROC eğrisi, dedektörün farklı eşik değerlerinde yapılan simülasyonlardaki tespit ve yanlış alarm oranlarını yansıtmaktadır. Gelen ölçümlerde aldatma olup olmaması ve filtrenin aldatma olup olmadığına karar vermesi kapsamında yapılan başarılı ve hatalı tespit kararları Şekil 3.14'te verildiği gibi alınmaktadır [65]. Aldatma sinyalleri varken aldatma kararı var tespitinin yapılabilmesi ve aldatma yokken yok kararının alınabilmesi başarılı bir tespit kararıdır. Öte yandan, aldatma yokken filtrenin aldatma var kararı alması yanlış alarm, aldatma varken aldatma yok kararının alınması ise aldatma saldırısı sinyalinin kaçırılmış olmasını ifade etmektedir.



Şekil 3.14: Filtrenin başarılı ve hatalı tespit kararları

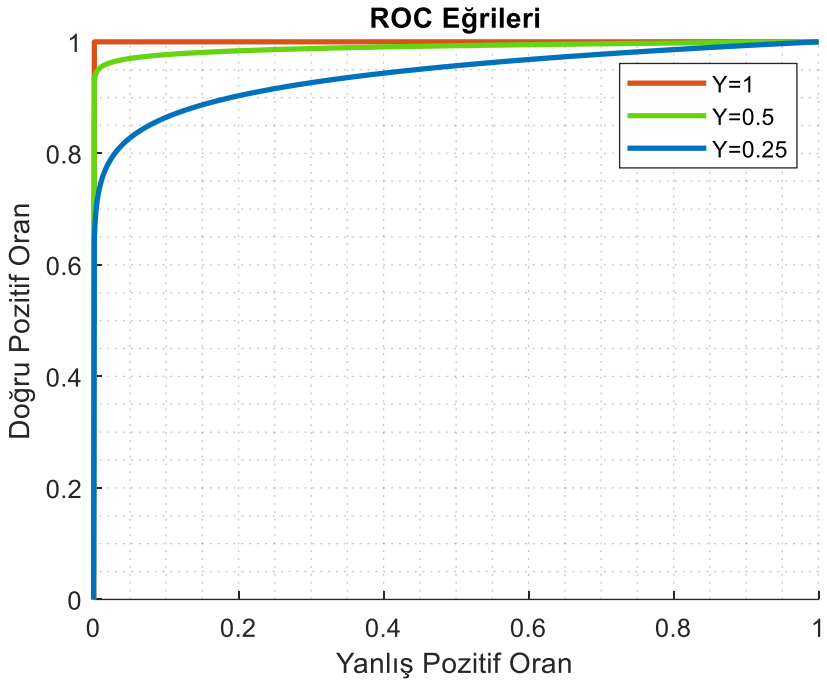
Yapılan simülasyonlarda, filtrenin aldatma tespitleri Şekil 3.14'te tanımlanan bölgelerden birine denk gelmektedir. 1000 koşuluk Monte-Carlo simülasyonları ile olası tüm aldatma senaryoları uygulanmış, bu simülasyonlardaki doğru pozitif oran ve yanlış pozitif oran değerleri Eşitlik (3.7) ve Eşitlik (3.8)'de verildiği gibi hesaplanmıştır [66].

$$Doğru\ Pozitif\ Oran = \frac{Gerçek\ Pozitif}{Gerçek\ Pozitif\ + Yanlış\ Negatif} \tag{3.7}$$

$$Yanlış\ Pozitif\ Oran = \frac{Yanlış\ Pozitif}{Yanlış\ Pozitif\ + Gerçek\ Negatif} \tag{3.8}$$

Eşitlik (3.7) ve Eşitlik (3.8)'de belirtilen oranların hesaplanması, ROC eğrisi üzerinde bir noktayı ifade etmektedir. Filtrenin farklı eşik değerleri (10, 15, 20, 25, 30, 35, 40, 45, 50, 55) için simülasyonlar tekrarlanmış, elde edilen bu noktaların birleştirilmesi ile Şekil 3.15'te de görüldüğü gibi ROC eğrisi çizdirilmiştir.

Y=1, Y=0.5, Y=0.25 katsayıları ile oluşturulan aldatma yörüngelerinde, farklı eşik değerleri ile simülasyonların yapılması sayesinde Şekil 3.15'teki gibi 3 farklı ROC eğrisi elde edilmiştir. Burada, KKS'ler üzerinde uygulanabilecek olası bütün aldatma senaryoları değerlendirilmiştir. Görüldüğü üzere, Y=1 ile oluşturulan aldatma saldırısı yörüngesi için, filtrenin aldatma tespit başarımı en yüksektir. Aldatma yörüngeleri daraldıkça, KKS ve ANS konumlama çözümleri birbirlerine daha da yaklaştığından aldatma tespit performansları azalmaktadır.



Şekil 3.15: Farklı yörüngeler için ROC eğrileri

ROC grafiklerinin altında kalan alan, dedektörün tespit performansını belirlemekte olup; Y=1, Y=0.5, Y=0.25 katsayılı aldatma yörüngeleri için, bu alanlar sırasıyla 0.9985, 0.9885, 0.9393 olarak hesaplanmıştır. Oluşturulan aldatma yörüngeleri daraldıkça eğrilerin altında kalan alanların da azaldığı, yani filtrenin aldatma tespit performansının azaldığı görülmektedir.

4. SONUÇ VE ÖNERİLER

KKS alıcıları tarafından, aldatma saldırılarının tespit edilebilmesi için literatürde pek çok farklı yöntem bulunmaktadır. Bu yöntemler alıcı yapısının farklı bloklarında tespitinin yapılması esasına dayalı olabilmektedir. Alıcı içerisinde kullanılan aldatma tespit ve karşı tedbir yöntemlerinin artırılması ile alıcının aldatmaya karşı performansının artması da sağlanabilmektedir. Bu tez çalışması kapsamında, KKS alıcısının pozisyon tahminini üretmeden hemen önceki navigasyon bloğunda kullanılmak üzere; farklı konumlama sistemlerinden gelen konumlama bilgilerinin füzyonunu yaparken, eş zamanlı olarak da aldatma tespit ve karşı tedbiri yapan bir Kalman filtresi tasarımı sunulmuştur. Alıcı yapısının önceki bloklarında aldatma tespit yöntemleri uygulanmış olmasına rağmen aldatmanın tespit edilememiş olması ihtimaline karşı, alıcının son bloğunda uygulanması önerilen bu yöntem ile alıcının aldatmaya karşı performansının artırılması amaçlanmıştır.

Yapılan çalışmaların ilk kısmı 2. bölümde anlatılmıştır. Bu bölümde, GPS, Galileo, GLONASS, BeiDou sistemlerini kullanarak konumlama çözümü üreten bir KKS alıcısı ile navigasyonu sağlayan insansız bir araç için aldatma tespiti ve aldatmaya karşı önlem için bir Kalman filtresi tasarımı sunulmuştur. Sırasıyla tüm KKS'ler üzerinde aldatma saldırılarının uygulandığı senaryolar altında Monte-Carlo simülasyonları yapılarak, filtrenin performansı yüzde tespit başarımı ve tespit süresi parametreleri ile değerlendirilmiştir.

Tezin 3. bölümünde, 2. bölümde kullanılan sisteme ek olarak bir ivmeölçer dahil edilerek ANS çözümleri filtreye eklenmiştir. Böylelikle, eş zamanlı olarak birden fazla KKS üzerinde aldatmanın uygulanabilir olduğu senaryolar altında da çalışan bir filtre tasarımı sunulmuştur. 4 farklı KKS ile uygulanabilecek olan tüm senaryolar için filtrenin başarılı bir şekilde aldatma tespit ve karşı önleminin yapıldığı gözlenmiştir. KKS'lerin pozisyonlama doğrulukları ile filtrenin başarım performansı ve tespit süresi arasındaki ilişkiler verilmiş, uygulanan aldatma senaryosundaki baskın ve resesif olan KKS'lerin pozisyon doğrulukları ile tespit süreleri arasındaki ilişki açıklanmıştır. Filtrenin farklı eşik değerleriyle ve farklı aldatma yörüngeleri ile Monte-Carlo

simülasyonları yapılarak, filtrenin aldatma tespit performansı ROC eğrileri ile incelenmiştir. Aldatma yörüngeleri daraldıkça aldatma tespit performansının azaldığı görülmüştür.

Bu tez çalışmasının literatüre temel katkısı; [52] referanslı bildiride sensör tümleşimi ve sensör ölçümlerindeki anlık hataların tespit edilerek elenebilmesi için önerilen yaklaşımın geliştirilerek, aldatma saldırısı tespit ve aldatmaya karşı tedbir amacıyla, KKS alıcıları içerisine uyarlanmasıdır. Referans alınan bu bildiri çalışmasındaki yaklaşım, tezin 2. bölümünde farklı küresel konumlama sistemleri ölçümleri için olacak şekilde düzenlemiş, anlık sensör ölçüm hataları tespiti yerine aldatma saldırısı tespiti amacına yönelik olacak şekilde güncellenmiştir. Tezin 3. bölümünde ise, ivmeölçer ölçümlerinin de aldatma tespiti yapılabilmesi için sisteme dahil edilerek geliştirilmesi katkısı eklenmiştir.

Bu çalışma kapsamında önerilen algoritma, geleneksel Kalman filtresi yaklaşımı ile aracın pozisyon ve hız tahminlerini oluşturarak aldatma tespit ve aldatmaya karşı tedbiri incelemiştir. Kalman filtresi, doğrusal sistemler için çalışabilir bir yöntemdir ve doğrusal olmayan sistemler için genişletilmiş Kalman filtresi (extended Kalman filter, EKF) gibi her zaman adımında sistemi doğrusallaştırmaya dayalı yöntemler kullanılmaktadır. Önerilen algoritma, doğrusal hareket modellemesi varsayımı ile tasarlanmıştır. Dolayısıyla, doğrusal olmayan hareket modelleri için algoritmanın EKF yaklaşımına uyarlanması önerilmektedir [67].

Önerilen Kalman filtresi algoritması, aldatma tespiti yapıldığını söyleyebilmek için maksimum yüzde başarım ve minimum tespit süresi ile karar verebilecek önceden belirlenmiş bir eşik değerini kullanmaktadır. Bu eşik değerinin sabit olarak belirlenmesi yerine, sabit yanlış alarm oranı (SYAO / constant false alarm rate, CFAR) gibi adaptif olarak değişebilen bir eşik değeri belirlenmesi yöntemi ile çalışmaların geliştirilmesi sağlanabilir [68]. Sistemin ve ortamın dinamiğine uyumlu olarak eşik değerinin seçilmesi sayesinde daha yüksek tespit performansları elde edilebilir.

Yukarıdaki gelecek çalışma önerilerine ek olarak, küresel konumlama sistemleri temelinde incelenen yaklaşımının KKS uydu sinyalleri seviyesinde olacak şekilde genişletilmesi önerilebilir. Ayrıca, tasarlanan Kalman filtresi algoritmasının gerçek ortamda, farklı araçlar, farklı aldatma yörüngeleri ve farklı aldatma senaryoları ile test

edilmesi önerilmektedir. Öte yandan, KKS alıcıları içerinde kullanılabilecek diğer aldatma tespit ve karşı önlem yöntemleri ile entegre kullanılarak performansının arttırılması da önerilmektedir.

KAYNAKLAR

[1] **Hofmann-Wellenhof, B., Lichtenegger, H., Collins, J.,** (2012). Global Positioning System Theory and Practice, New York: Springer Science & Business Media.

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

[3] **Cheng, C. H.,** (1998). Calculations for Positioning with the Global Navigation Satellite System, in *Doctoral dissertation, Ohio University*, Ohio.

[4] **Gaglione, S., Angrisano, A., Freda, P., Innac, A., Vultaggio, M., Crocetto**, **N.,** (2015). Benefit of GNSS multiconstellation in position and velocity domain, *IEEE Metrology for Aerospace (MetroAeroSpace),* 9-15.

[5] **The Royal Academy of Engineering,** (2011). Global Navigation Space Systems: reliance and vulnerabilities, *London*.

[6] **Ioannides, R. T., Pany, T., Gibbons, G.,** (2016). Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques, *Proceedings of the IEEE,*104.6: 1174-1194.

[7] **Stenberg, N., Axell, E., Rantakokko, J., Hendeby, G.,** (2020). GNSS spoofing mitigation using multiple receivers, *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS),* 555-565.

[8] **Zhang, J., Cui, X., Xu, H., Zhao, S., Lu, M.,** (2018). Efficient signal separation method based on antenna arrays for GNSS meaconing, *Tsinghua Science and Technology,* vol. 24, no. 2, 216-225.

[9] **Bethi, P., Pathipati, S., Aparna, P.,** (2020). Stealthy GPS Spoofing: Spoofer Systems, Spoofing Techniques and Strategies, *2020 IEEE 17th India Council International Conference (INDICON),*1-7.

[10] **İçen, E.,** (2018). Küresel ve Bölgesel Konumlama Sistemleri, Teknolojileri ve Uygulamaları, *Ulaştırma, Denizcilik ve Haberleşme Bakanlığı / Havacılık ve Uzay Teknolojileri Genel Müdürlüğü*.

[11] "Space Segment: Constellation Arrangement," GPS.gov, [Online]. Available: https://www.gps.gov/systems/gps/space/. [Accessed 20 03 2023].

[12] "Galileo satellites," The European Space Agency (ESA), [Online]. Available: https://www.esa.int/Applications/Navigation/Galileo/Galileo_satellites. [Accessed 20 03 2023].

[13] C. S. I. Center, "Global Navigation Satellite System: GLONASS Interface Control Document," 1998. [Online]. Available: https://www.unavco.org/help/glossary/docs/ICD_GLONASS_4.0_(1998)_en.pdf. [Accessed 20 03 2023].

[14] "BeiDou Navigation Satellite System," BeiDou, 2020. [Online]. Available: http://en.beidou.gov.cn/SYSTEMS/ICD/. [Accessed 20 03 2023].

[15] **El-naggar, A. M.,** (2011). An alternative methodology for the mathematical treatment of GPS positioning, *Alexandria Engineering Journal,* vol. 50, no. 4, 359-366.

[16] **Roongpiboonsopit, D., Karimi, H. A.,** (2009). A Multi-Constellations Satellite Selection Algorithm for Integrated Global Navigation Satellite Systems, *Journal of Intelligent Transportation Systems,* vol. 13, no. 3, 127-141.

[17] **Sadman, A. A. M. S., Hossam-E-Haider, M.,** (2019). GNSS Position Accuracy Considering GDOP and UERE for Different Constellation over Bangladesh, *22nd International Conference on Computer and Information Technology (ICCIT),*1-5.

[18] **Akos, D. M.,** (2012). Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC), *NAVIGATION: Journal of the Institute of Navigation,* vol. 59, no. 4, 281-290.

[19] **El-Rabbany,** (2002). Introduction to GPS: The Global Positioning System, Artech House.

[20] **Mutlu, B.,** (2011). Tek Frekanslı GPS Alıcı ile Hassas Konum Belirleme, *Jeodezi ve Fotogrametri Mühendisliği Anabilim Dalı Yüksek Lisans Tezi, Gebze*.

[21] **Setti, P. D. T., Alves, D. B. M., Silva, C. M. D.,** (2019). Klobuchar and Nequick G ionospheric models comparison for multi-GNSS single-frequency code point positioning in the Brazilian region, *Boletim de Ciencias Geodesicas,* vol. 25, no. 3.

[22] **Özuğur, İ., Yurt, K.,** (2020). Comparison of Troposphere Models Used in Commercial GPS Softwares, *Turkish Journal of Geosciences,* vol. 1, no. 2, 63-71.

[23] **Kamatham, Y.,** (2018). Estimation, Analysis and Prediction of Multipath Error for Static GNSS Applications, *2018 Conference on Signal Processing And Communication Engineering Systems (SPACES),* 62-65.

[24] **Mekik, C., Can, O.,** (2010). Multipath Effects in RTK GPS and A Case Study, *Journal of Aeronautics, Astronautics and Aviation, Series A,* vol. 42, no. 4, 231-240.

[25] **Langley, R. B.,** (1997). GPS Receiver System Noise, *GPS World,* vol. 8, no. 5, 40-45.

[26] **Bellad, V., Petovello, M. G., Lachapelle, G.,** (2014). Characterization of Tracking and Position Errors in GNSS Receivers with Intermittent Tracking, *Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014),* 2698-2712.

[27] **Akan, Ş. T.,** (2020). MEMS Ataletsel Ölçüm Birimi Stokastik Hata Parametrelerinin Tanılanması ve Kestirimi, *Hacettepe Üniversitesi, Elektrik ve Elektronik Mühendisliği, Yüksek Lisans Tezi, Ankara*.

[28] **Güreş, O.,** (2019). Development and Comparison of the Extended Kalman Filter and Unscented Kalman Filter for Both Tightly Coupled and Loosely Coupled INS/GNSS Integration By Using MEMS IMU,

Electrical and Electronics Engineering Department, Middle East Technical University, Ankara.

[29] **Godha, S.,** (2006). Performance Evaluation of Low Cost MEMS-Based IMU Integrated With GPS for Land Vehicle Navigation Application, *Department of Geomatics Engineering, University of Calgary, Calgary, Alberta*.

[30] **Jonsson, C.,** (2016). Velocity estimation in land vehicle applications; Sensor Fusion using GPS, IMU and Output-shaft, *Royal Institute of Technology, School of Engineering Sciences, Aerospace Engineering, Stockholm, Sweden.*

[31] **Peng, K.-Y., Lin, C.-A., Chian, K.-W.,** (2012). The Performance Analysis of An AKF Based Tightly-Coupled INS/GPS Integrated Positioning and Orientation Scheme with Odometer and Non-Holonomic Constraints, *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences,* vol. 39, 481-486.

[32] **Cai, G., Chen, B. M., Lee, T. H.,** (2011). Coordinate Systems and Transformations, *Unmanned Rotorcraft Systems. Advances in Industrial Control*, London, Springer, 23-34.

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

[34] **Shepard, D. P., Bhatti, J. A., Humphreys, T. E.,** (2012). AVIATION: Signal Spoofing - Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle. [Online]. Available: https://radionavlab.ae.utexas.edu/images/stories/files/papers/drone_hack_shepard.pdf. [Accessed 20 03 2023].

[35] I. GNSS, Reports of Mass GPS Spoofing Attack in the Black Sea Strengthen Calls for PNT Backup, 24 07 2017. [Online]. Available: https://insidegnss.com/reports-of-mass-gps-spoofing-attack-in-the-black-sea-strengthen-calls-for-pnt-backup/. [Accessed 20 03 2023].

[36] **Junzhi, L., Wanqing, L., Qixiang, F., Beidian, L.,** (2019). Research Progress of GNSS Spoofing and Spoofing Detection Technology, *2019 IEEE 19th International Conference on Communication Technology (ICCT),* 1360-1369.

[37] **Ahmad, M., Farid, M. A., Ahmed, S., Saeed, K., Asharf, M., Akhtar, U.,** (2019). Impact and Detection of GPS Spoofing and Countermeasures against Spoofing, *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET),* 1-8.

[38] **Manfredini, E. G., Akos, D. M., Chen, Y.-H., Lo, S., Walter, T., Enge**, **P.,** (2018). Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers, *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation,* 672-689.

[39] **Zhou, M., Fan, C., Chen, D., Mao, C.,** (2010). A compact automatic gain control loop for GNSS RF receiver, *2010 10th IEEE International Conference on Solid-State and Integrated Circuit Technology,* 284-286.

[40] **Üstündağ, M. B.,** (2023). Global Positioning System Spoofing and Detection Techniques, *Middle East Technical University, Ankara*.

[41] **Cao, K., Hu, Y., Xu, J., Li, B.,** (2013). Research On Improved RAIM Algorithm Based On Parity Vector Method, *2013 International Conference on Information Technology and Applications,* 221-224.

[42] **Sun, Y., Fu, L.,** (2019). A New Threat for Pseudorange-Based RAIM: Adversarial Attacks on GNSS Positioning, *IEEE Access,* vol. 7, 126051-126058.

[43] **Zhang, K., Papadimitratos, P.,** (2019). Secure Multi-constellation GNSS Receivers with Clustering-based Solution Separation Algorithm, *2019 IEEE Aerospace Conference,* 1-9.

[44] **Broumandan, A., Lachapelle, G.,** (2018). Spoofing Detection Using GNSS/INS/Odometer Coupling for Vehicular Navigation, *Sensors,* vol. 18, no. 5, 1305.

[45] **Dasgupta, S., Rahman, M., Islam, M., Chowdhury, M.,** (2022). A Sensor Fusion-Based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles, *IEEE Transactions on Intelligent Transportation Systems,* vol. 23, no. 12, 23559 - 23572.

[46] **Grejner-Brzezinska, D. A., Toth, C. K., Moore, T., Raquet, J. F., Miller, M. M., Kealy, A.,** (2016). Multisensor Navigation Systems: A Remedy for GNSS Vulnerabilities?, *Proceedings of the IEEE,* vol. 104, no. 6, 1339-1353.

[47] **Akçay, H. I., Onat, E.,** (2022). Position and Velocity Detection with RADAR and GPS Fusion, *30th Signal Processing and Communications Applications Conference (SIU),* 1-4.

[48] **Welch, G., Bishop, G.,** (1995). An Introduction to the Kalman Filter, *Department of Computer Science, University of North Carolina at Chapel Hill*.

[49] **Silva, V., Parkes, S. M.,** (2003). On the Design of an Optimal GNC Sensor Architecture for Autonomous Planetary Landers, *DASIA 2003-Data Systems in Aerospace,* vol. 532.

[50] **Beşdok E., Özçelik, A. E.,** (2009). Kalman Filtreleme Yöntemiyle Otonom Hava Araç Navigasyonunda GPS/INS Entegrasyonu, *TMMOB Harita ve Kadastro Mühendisleri Odası, 12. Türkiye Harita Bilimsel ve Teknik Kurultayı, Ankara*.

[51] **Zhang, M., Liu K., Li, C.,** (2016). Unmanned Ground Vehicle Positioning System by GPS/Dead-Reckoning/IMU Sensor Fusion, *Proceedings of the 2nd Annual International Conference on Electronics, Electrical Engineering and Information Science (EEEIS 2016),* vol. 117, 737-747.

[52] **Gingras, D.,** (2009). An Overview of Positioning and Data Fusion Techniques Applied to Land Vehicle Navigation Systems, *Automotive Informatics and Communicative Systems: Principles in Vehicular Networks and Data Exchange,* 219-246.

[53] **Reuper, B., Becker M., Leinen, S.,** (2018). Benefits of Multi-Constellation /Multi-Frequency GNSS in a Tightly Coupled GNSS/IMU/Odometry Integration Algorithm, *Sensors,* vol. 18, no. 9, 3052.

[54] **Falco, G., Pini M., Marucco, G.,** (2017). Loose and Tight GNSS/INS Integrations: Comparison of Performance Assessed in Real Urban Scenarios, *Sensors,* vol. 17, no. 2, 255.

[55] **Mosavia, M. R., Tabatabaeia A., Zandib, M. J.,** (2016). Positioning Improvement by Combining GPS and GLONASS Based on Kalman Filter and Its Application in GPS Spoofing Situations, *Gyroscopy and Navigation,* vol. 7, no. 4, 318-325.

[56] **Tanıl, Ç., Khanafseh, S., Joerger M., Pervan, B.,** (2018). An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position, *IEEE Transactions on Aerospace and Electronic Systems,* vol. 54, no. 1, 131-143.

[57] **Liu, Y., Li, S., Fu, Q., Liu Z. Zhou, Q.,** (2019). Analysis of Kalman Filter Innovation-Based GNSS Spoofing Detection Method for INS/GNSS Integrated Navigation System, *IEEE Sensors Journal,* vol. 19, no. 13, 5167-5178.

[58] **Zhang, L., Zhao, H., Sun, C., Bai L., Feng, W.,** (2022). Enhanced GNSS Spoofing Detector via Multiple-Epoch Inertial Navigation Sensor Prediction in a Tightly-Coupled System, *IEEE Sensors Journal,* vol. 22, no. 9, 8633-8647.

[59] **Dasgupta, S., Rahman, M., Islam M., Chowdhury, M.,** (2022). A Sensor Fusion-based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles, *IEEE Transactions on Intelligent Transportation Systems,* vol. 23, no. 12, 23559-23572.

[60] "Model IMU, GPS, and INS/GPS," MathWorks, [Online]. Available: https://www.mathworks.com/help/fusion/gs/model-imu-gps-and-insgps.html. [Accessed 20 03 2023].

[61] U-Blox, "NEO-M8 U-Blox M8 Concurrent GNSS Modules Data Sheet," [Online]. Available: https://content.u-blox.com/sites/default/files/NEO-M8-FW3_DataSheet_UBX-15031086.pdf. [Accessed 20 03 2023].

[62] **Akçay, H. I., Onat, E.,** (2022). Kalman Filter Design For Spoofing Detection and Anti-Spoofing in GNSS Receivers, *10th International Conference on Advanced Technologies (ICAT)*.

[63] "Inertial Sense IMX-5 Datasheet," Inertial Sense, 03 06 2023. [Online]. Available: https://docs.inertialsense.com/datasheets/IMX-5_IMU_AHRS_GNSS-INS_Datasheet.pdf. [Accessed 20 03 2023].

[64] **Walchko, K. J., Nechyba, M. C., Schwartz E., Arroyo, A.,** (2003). Embedded Low Cost Inertial Navigation System, *Florida Conference on Recent Advances in Robotics,* 8-9.

[65] **Maxion R. A., Roberts, R. R.,** (2004). Proper Use of ROC Curves in Intrusion/Anomaly Detection, *School of Computing Science, Technical Report Series.*

[66] **Latecki, L. J., Lazarevic, A., Pokrajac, D.,** (2007). Outlier Detection with Kernel Density Functions, *Machine Learning and Data Mining in Pattern Recognition, 5th International Conference, MLDM 2007,* vol. 7, 61-75.

[67] **Awasthi, V., Raj, K.** (2011). A Comparison of Kalman Filter and Extended Kalman Filter in State Estimation, *International Journal of Electronics Engineering,* vol. 3, no. 1, 67-71.

[68] **Chen, X., Hu M., Lu, S.,** (2022). Modelling and Analysis of Constant False Alarm Rate Performance in Presence of Jamming Environments, *Mathematical Problems in Engineering,* 1-11.