İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

OTOMATİK BAĞIMLI GÖZETİM-YAYINI GÜVENLİK ANALİZİ

YÜKSEK LİSANS TEZİ

Eren KOCAAĞA

Bilgi Güvenliği Mühendisliği ve Kriptografi

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

Tez Danışmanı: Doç. Dr. M. Oğuzhan KÜLEKCİ

05 Mayıs 2017

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

OTOMATİK BAĞIMLI GÖZETİM-YAYINI GÜVENLİK ANALİZİ

YÜKSEK LİSANS TEZİ

Eren KOCAAĞA
(707151009)

Bilgi Güvenliği Mühendisliği ve Kriptografi

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

Tez Danışmanı: Doç. Dr. M. Oğuzhan KÜLEKCİ

05 Mayıs 2017

İTÜ, Bilişim Enstitüsü'nün 707151009 numaralı Yüksek Lisans Öğrencisi Eren KOCAAĞA, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "OTOMATİK BAĞIMLI GÖZETİM-YAYINI GÜVENLİK ANALİZİ" başlıklı tezini aşağıdaki imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Doç. Dr. M. Oğuzhan KÜLEKCİ** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Doç. Dr. Mustafa Ersel KARMAŞAK** İstanbul Teknik Üniversitesi	.....
	Dr. Gülay KAPLAN TÜBİTAK BİLGEM	.....
		.....

Teslim Tarihi : **5 Mayıs 2017**
Savunma Tarihi : **16 Haziran 2017**

Kan kardeşim
Şehit Polis Çağdaş ARSLAN'a,

ÖNSÖZ

Öncelikle tez konusunu seçerken isteklerimi göz önünde bulundurup bana yardımcı olan tez danışmanım Doç.Dr. M. Oğuzhan KÜLEKCİ'ye teşekkürlerimi sunarım. Kaynak aramak için yardım talep ettiğim TÜBİTAK BİLGEM BTE'de çalışan Radar ekibine, bu süreçte benden desteğini bir an için bile esirgemeyen değerli dostlarım, Alperen DEDEOĞLU ve Çağ ÇETİN'e, tüm eğitim hayatım boyunca benden maddi ve manevi desteklerini esirgemeyen, her zaman yanımda olan sevgili babam, annem ve kardeşime teşekkürlerimi bir borç bilirim.

05 Mayıs 2017

Eren KOCAAĞA
Araştırmacı

İÇİNDEKİLER

Sayfa

KISALTMALAR

ACK : Onay Mesajı
ADS : Otomatik Bağımlı Gözetim
ADS-B : Otomatik Bağımlı Gözetim Yayını
ASTERIX : Tüm Amaçlı Yapısal EUROCONTROL Radar Bilgi Alışverişi
ATM : Hava Trafik Yönetimi
CA : Sertifika Otoritesi
CASCADE : Gözetim ve Yayın Haberleşme Uygulamaları
CNS : Haberleşme, Seyrüsefer ve Gözetleme
DHMİ : Devlet Hava Meydanları İşletmesi
DME : Mesafe Ölçüm Cihazları
DoS : Hizmetin Engellenmesi
ECC : Eliptik Eğri Şifreleme
ECDSA : Eliptik Eğri Veri İmzalama Algoritması
FAA : Federal Havacılık İdaresi
FANS : Geleceğin Hava Seyrüsefer Sistemleri
PRF : Darbe Tekrarlama Frekansı
FRUIT : Eşzamanlı Olmayan Yanıtlar
GNSS : Global Navigasyon Uydu Sistemi
GPS : Global Konumlandırma Sistemi
ICAO : Uluslararası Havacılık Örgütü
ILS : Gösterge İniş Sistemi
MAC : Mesaj Kimlik Doğrulama Kodu
MLAT : Çok Taraflı Gözetim
MSSR : Tek Darbe İkincil Gözetim Radarı
NextGen : Yeni Nesil Havacılık Sistemi
PKI : Açık Anahtarlı Kriptografik Yöntemler
PPM : Darbe Konum Modülasyonu
PSR : Birincil Gözetim Radarı
SMR : Yüzey Hareketi Radarı
SMS : Emniyet YÖnetim Sistemleri
SPI : Özel Amaçlı Kimlik
SSR : İkincil Gözetim Radarı
SYN : Senkronizasyon Mesajı
SYN-ACK : Senkronizasyon-Onay Mesajı
TACAN : Taktik Hava Navigasyonu
TCAS : Trafik Çarpışma Kaçınma Sistemi
TDL : Taktik Veri Bağlantısı
TDOA : Varış Zaman Farkı
TESLA : Zamana Uygun Verimli Akış Kaybı Toleranslı Kimlik Doğrulama
TOA : Varış Zamanı
VOR : Çok Yönlü Radyo Aralığı

SEMBOLLER

$\mathbf{P_s}$	**:** Radardan gönderilen güç [W]
$\mathbf{P_r}$	**:** Yansıyan güç [W]
$\mathbf{S_u}$	**:** Dağıtık güç yoğunluğu
$\mathbf{S_g}$	**:** Yönlendirilmiş enerji yoğunluğu
R	**:** Anten hedef menzili
G	**:** Anten kazancı
ϕ	**:** Radar kesiti
$\mathbf{N_P}$, $\mathbf{N_V}$	**:** Rasgele bit dizisi
$\mathbf{t_d}$	**:** Gecikmeler toplamı
$\mathbf{t_p}$	**:** Dalganın ulaşma süresidir
c	**:** Işık hızı

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

OTOMATİK BAĞIMLI GÖZETİM-YAYINI GÜVENLİK ANALİZİ

ÖZET

Devlet Hava Meydanları İşletmesi istatistiklerine göre 2016 yılında Türkiye havalimanlarında yolcu, yük ve ticari uçaklar dahil olmak üzere toplam 1.829.028 uçak ve 173.959.159 yolcu trafiği gerçekleşmiştir. 2019 yılı için öngörü bu rakamların yaklaşık yüzde 25 daha fazlasıdır. Bu denli yüksek rakamların geçtiği uçak trafiğinde yeni jenerasyon uçuş kontrol sisteminin en önemli adımı olan Otomatik Bağımlı Gözetim-Yayını(ADS-B)'nda kullanılan haberleşme protokolündeki güvenlik açıkları, hem sivil hem de askeri uçuşlar için tehlikeli riskler barındırmaktadır.

Bilgi güvenliği alanındaki bilgi sistemlerinin artan kullanımı nedeniyle siber güvenlik, havacılık ve güvenlik açıkları arasındaki ilişkinin kapsamlı bir literatür taraması yapılmıştır. Sivil havacılık, yeni teknolojilerin devreye sokulması yoluyla hava trafiği yönetim sisteminin gelişim sürecindedir. Dolayısıyla, havacılık haberleşmesinin modernizasyonu henüz giderilmemiş birtakım güvenlik sorunlarını yaratmaktadır. Çalışmanın amacı Otomatik Bağımlı Gözetim Yayına karşı siber saldırıların sistematik bir şekilde okuyucuya tanıtmak ve niteliksel güvenlik analizini yapmaktır. Bu tez, havacılıkta siber güvenlik tehditlerinin etkisini anlamak için bir referans kılavuzu olarak ve haberleşme protokolünün neden olduğu güvenlik sorunlarıyla yüzleşmek, bilinçlendirmek ve uzmanlık seviyesini artırmak için kullanılabilir.

Bu çalışmada, ADS-B teknolojisinin güvenlik analizi, atak çeşitleri yöntemlerine göre sınıflandırılarak okuyucuya sunulmuştur. ADS-B teknolojisini güvenli hale getirmek için bir dizi metodlar karşılaştırmalı olarak anlatılmış, uygulanabilirlikleri hakkında yorumlar yapılmıştır.

AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST SECURITY ANALYSIS

SUMMARY

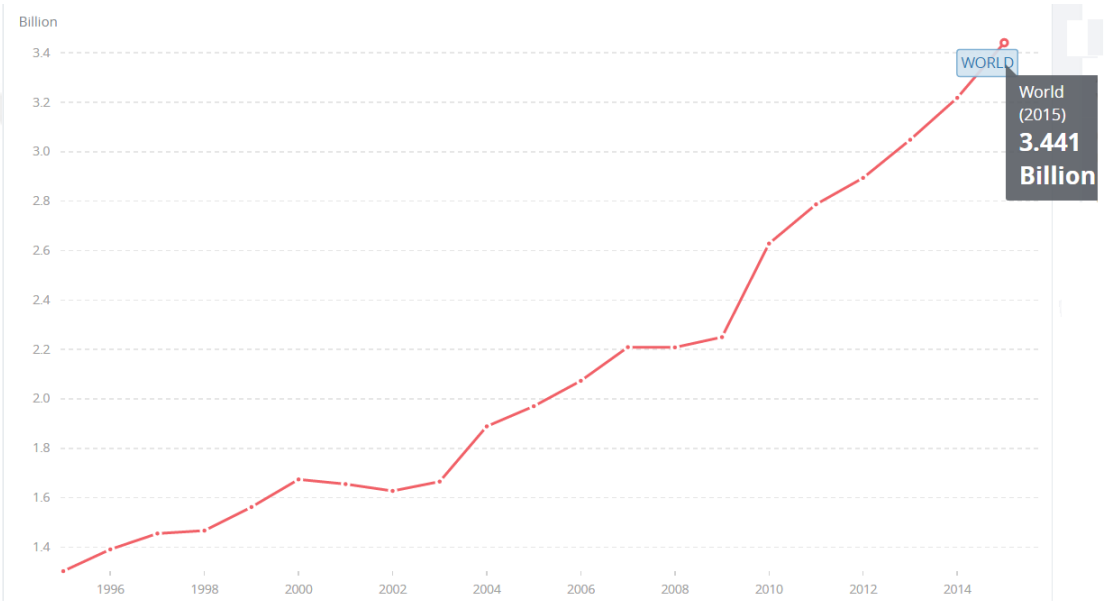
According to DHMI statistics, a total of 1,829,028 airplane (including passenger aircraft, freight aircraft and commercial aircraft) and 173,959,159 passengers were transported at Turkish airports in 2016. The forecast for 2019 is about 25 percent more than these figures. Vulnerabilities in the communication protocol used in Auto-Dependent Surveillance (ADS-B), the most important unit of NextGen, called the new generation flight control system in aircraft traffic where exists such high numbers, present dangerous risks for both civilian and military flights.

Due to the increasing use of information systems in the field of information security, a comprehensive literature search of the relationship between cyber security, aviation and security vulnerabilities has been conducted. Civil aviation is in the development stage of the air traffic management system through the introduction of new technologies. For this reason, the modernization of aviation communication is creating some security problems that have not yet been solved. The purpose of this thesis is to systematically introduce cyber attacks against the Automatic Dependent Surveillance Broadcast to the reader and conduct a qualitative security analysis. This thesis can be used as a reference guide to understand the effects of cyber security threats in aviation and can be used to face security problems caused by the communication protocol, raise awareness and increase the level of expertise.

In this study, the security analysis of ADS-B technology is presented to the reader by classifying it according to attack types. A number of methods have been described comparatively to make ADS-B technology secure, and comments on its applicability have been made.

1. GİRİŞ

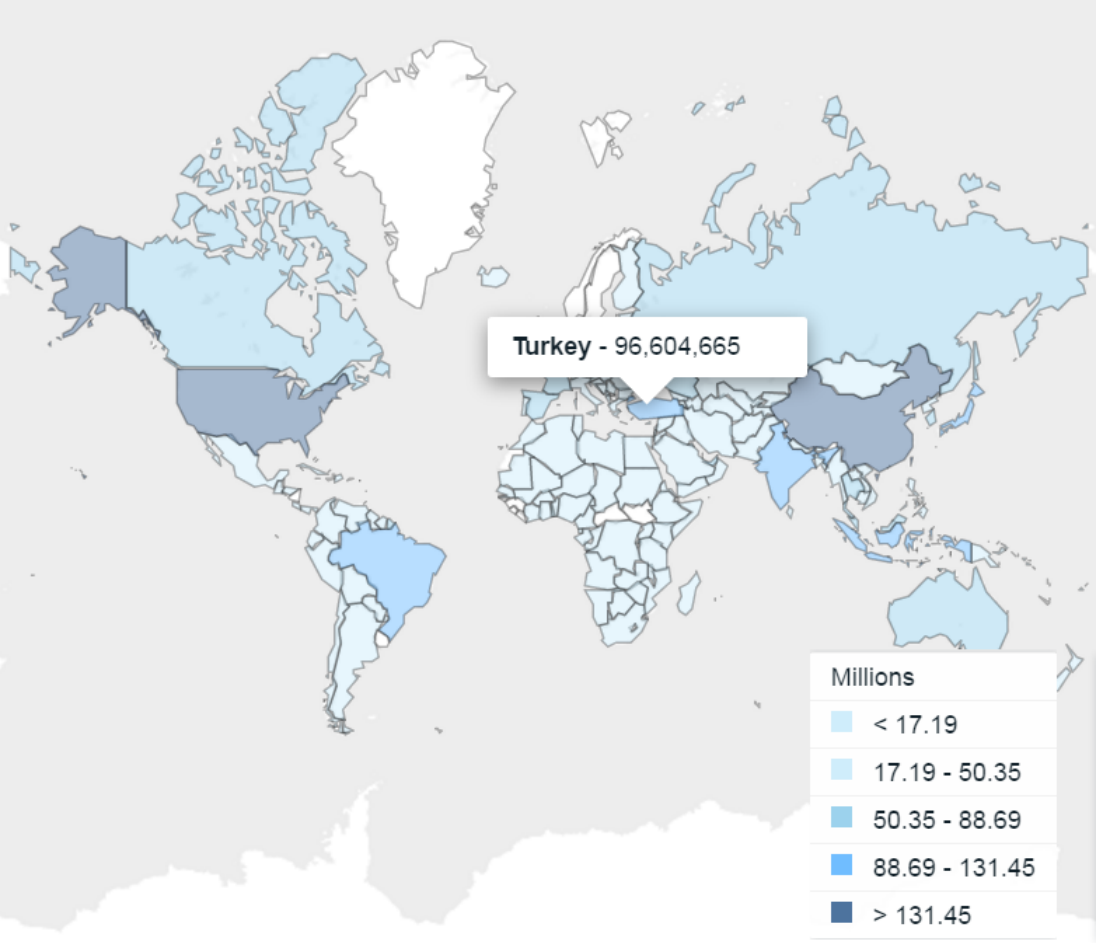
Hava taşımacılığına olan talep her geçen gün artmakta ve gelecekte büyümeye devam etmesi beklenmektedir. Federal Havacılık İdaresi (FAA)'nin yaptığı tahminlere göre, hava ulaşım yolcularının 2025 yılına kadar iki katına çıkması öngörülmekte ve mevcut hava taşımacılığı sisteminin gelecekteki talepleri karşılayamadığı düşünülmektedir [3].



Şekil 1.1 : 2000-2015 yılları hava taşımacılığı, yolcu sayısı [1].

Gelecekte artan talebe cevap olarak, kapasiteyi arttırmak ve güvenliği artırmak için yeni teknolojiler içeren Yeni Nesil Havacılık (NextGen) önerilmektedir [4]. Günümüzde NextGen teknolojisi uygulanmaya başlanmıştır. Şu anda geliştirilmekte olan NextGen teknolojilerinden biri, yeni bir uydu tabanlı gözetim teknolojisi olan Ortak Bağımlı Gözetim Yayını'dır (ADS-B). Bu tarz teknoloji geçişleri karmaşık sorunları çözmek için gereklidir. Ancak bazen mevcut bir teknolojiden yeni bir teknolojiye uygun bir geçiş yapmak zordur.

Emniyet Yönetim Sistemleri (SMS), bir sistemdeki gerçek zamanlı verileri incelemek ve izlemek için kullanılır. Bu veriler, kazaları azaltmak ve önlemek için analiz edilir [5]. Amaç mümkün olan en düşük kaza oranını elde etmek ve emniyetimizi sürekli iyileştirmektir [6]. Bu çalışmada havacılık güvenliği problemlerini öngörmek için



Şekil 1.2 : 2015 yılı hava taşımacılığı, yolcu sayısı.

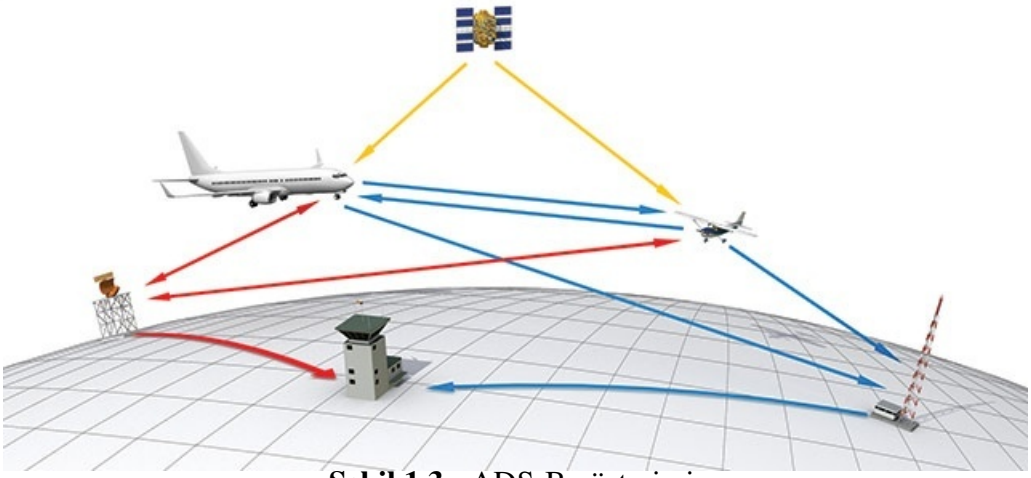
NextGen mimarisi analiz edilmekte ve genel güvenlik konularını ele alınıp ADS-B'nin güvenlik açıkları üzerinde durulmaktadır.

Otomatik Bagımlı Gözetim Yayını uçak trafiğini daha hassas bir şekilde¸ takip edebilme imkanı veren ve hava sahasını daha verimli kullanan güncel bir teknolojidir. İlgili uçağın hızı, yüksekliği ve uçağın dönme, tırmanma veya alçalma gibi diger verilerle birlikte sayısal veri hattı vasıtasıyla havadaki konumunu ADS-B'yle yayınlamaktadır. Hava trafik kontrol sistemine entegre edilmiş ve uçaklara yerleştirilen ADS-B alıcıları, havada ve yerde gerçek zamanlı havacılık trafiğini gerçeğe çok yakın betimlemektedir. Bu teknolojinin en önemli faydası pilotlara ve yer kontrolörlerinde gerçek zamanlı eş bilgi sunma yeteneğidir [4].

ADS-B, bir uçağın uzayda konumunu hassas şekilde belirlemek için uydu tabanlı global konumlandırma sistemine (GPS) güvenir. Sistem daha sonra, konumu uçağın türü, hızı, uçuş numarası ve dönüş, yükselme veya alçalma gibi diğer bilgilerle birleştirilen dijital bir koda çevirir. Bütün bu bilgileri içeren dijital kod, birkaç saniye

içinde güncellenir ve uçaklardan veri hattı adı verilen 1090 MHz frekansında yayınlar. Yaklaşık 240 kilometre içindeki diğer hava aracı ve yer istasyonları, veri yayınlarını alır ve bilgileri, kokpitteki pilotlar ve radar kulesindeki kontrolörler Hava Trafik Kontrol Gösterimi ekranında görürler. Seyrüsefer cihazları, ADS-B hedeflerini normal trafik ekranında diğer radar hedefleriyle birlikte görme imkanı sunar.

Türkiye'de ADS-B sistemlerin gerçeklenmesi adına ilk adım 2008 yılında EUROCONTROL ve Devlet Hava Meydanları Genel Müdürlüğü işbirliğiyle CASCADE (Cooperative ATS through Surveillance and Communication Applications Deployed in ECAC - ECAC Bölgesinde Gözetim ve Sesli İletişim Uygulamalarına Yönelik ATS İşbirliği) projesiyle atılmıştır. CASCADE projesi doğrultusunda ADS-B sistemleri 2 yıl boyunca Trabzon Havalimanı'nda başarılı bir şekilde test edilmiştir [7].



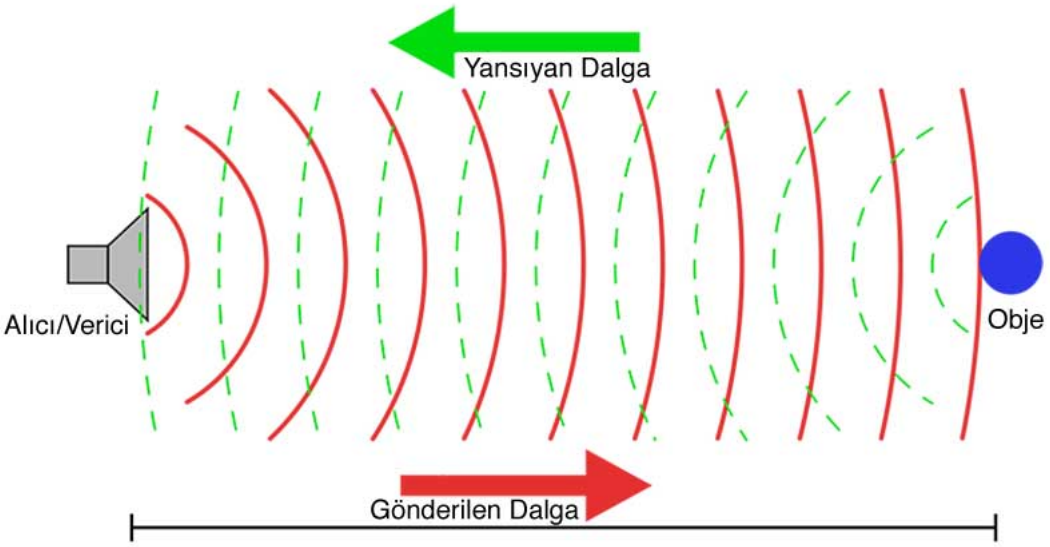
Şekil 1.3 : ADS-B gösterimi.

Bu çalışmada, ADS-B teknolojisi okuyuca tanıtılmakta ve ADS-B haberleşmesiyle ilişkili güvenlik açıkları incelenmektedir. Saldırıların ulusal hava sahası sistemi operasyonları üzerindeki potansiyel etkilerini incelemek için ataklar sınıflandırılmıştr. Bu sınıflandırma, risk analizi ve yönetimini destekleyen ADS-B uygulamasıyla ilişkili tehditlerin kapsamlı bir sekilde anlaşılmasına yardımcı olur.

1.1 Radarın Çalışma Prensibi

Radar, nesnelerin aralığını, açısını veya hızını belirlemek için radyo dalgalarını kullanan bir nesne algılama sistemidir. Uçak, gemi, uzay aracı, füzeler, motorlu taşıtlar, hava oluşumları ve arazi niteliklerini tespit etmek için kullanılabilir. Bir radar sistemi, radyo veya mikrodalga alanındaki elektromanyetik dalgaları üreten bir verici

anten, bir alıcı anten (genellikle verici ve alıcı için aynı anten kullanılır) ve nesnelerin özelliklerini belirleyen işlemci içerir. Vericiden gelen radyo dalgaları, hedef nesneden yansıyıp alıcıya geri dönmekte ve nesnenin konumu ve hızı hakkında bilgi vermektedir.



Şekil 1.4 : Radarın çalışma prensibi

Bir radar sistemi, önceden belirlenmiş yönde radar sinyalleri adı verilen radyo dalgalarını yayınlayan bir vericiye sahiptir. Yayınlanan radyo dalgaları bir cisimle temasa girdiğinde genellikle birçok yönde yansır ve dağılır. Vericiye doğru geri yansıtılan radar sinyalleri, radarı çalıştırmak için arzu edilen radar sinyalleridir. Nesne vericiye doğru hareket ediyorsa Doppler etkisinden dolayı radyo dalgalarının frekansında değişikliklere sahip olacaktır.

Radar alıcıları her zaman olmasa da genellikle vericiyle aynı yerde konuşlandırılır. Alıcı antenin yakaladığı yansıyan radar sinyalleri zayıf olsa dahi elektronik amplifikatörler ile güçlendirilebilir. Radar sinyallerinin güçlendirilip algılanabilmesi için daha karmaşık sinyal işleme yöntemleri de kullanılmaktadır.

Radyo dalgalarının geçtiği ortamın zayıf emilimi, radar setlerinin nispeten daha uzun aralıklarla radar setlerinin algılanmasını sağlayan aralıkları, yani görünür ışık, kızılötesi ışık ve ultraviyole ışığı gibi diğer elektromanyetik dalga boylarının çok güçlü bir şekilde zayıflatıldığını gösterir. Sis, bulutlar, yağmur, düşen kar ve görünür ışığı engelleyen karışıklık gibi hava olayları genellikle radyo dalgalarına karşı saydamdır. Algılama amaçları haricinde, radar tasarımı sırasında su buharı, yağmur damlası veya

atmosferik gazlar (özellikle oksijen) tarafından emilen veya dağılmış belirli radyo frekanslarından kaçınılmaktadır.

Hava ve karasal trafik kontrolü, radar astronomisi, hava savunma sistemleri, yer işaretlerini ve diğer gemileri bulmak için deniz radarları, uçak çarpma önleme sistemleri, okyanus gözetim sistemleri ve dış mekan gözetimi dahil, radarın modern kullanımı çok çeşitlidir [8].

1.2 Radar Denklemi

Radar denklemi radardan gönderilen enerjinin, dalganın yayılmasından başlayarak yansıyan sinyallerin alınmasına kadar geçen evredeki fiziksel ilişkilerini betimlemek için kullanılır. Bir radar setinin performansının değerlendirmesi de radar denklemi kullanılarak yapılır.

Elektromanyetik dalgaların ideal ortam şartlarında herhangi bozucu etkiler olmadan yayıldığını varsayımıyla, eğer yüksek frekanslı enerji izotropik bir vericiden yayın yapıyorsa enerji her yöne eşit dağılır. Eşdeğer güç yoğunluğuna sahip alanlar vericinin etrafında R yarıçapı uzaklığında alanı $A = 4\pi.R^2$ olan bir küreler oluşturur. Küre yarıçapı artıkça enerji daha geniş bir yüzeye dağılacağından birim alana düşen güç yoğunluğu azalmış olacaktır. Sanal bir yüzeyde kaynak ile yüzey arasındaki açıklık arttıkça ışıma ıraksayı (diverjansı) sonucu güç yoğunluğu azalır. Dağıtık güç yoğunluğu S_u formülü:

$$S_u = \frac{P_s}{4.\pi.R^2} \tag{1.1}$$

P_s: gönderilen güç $[W]$
S_u: dağıtık güç yoğunluğu
R: anten-hedef menzili $[m]$

Eğer yayın (gönderim gücü sabit iken) kürenin belli sınırlı bir bölgesine tasnif edilmiş ise o bölgede güç yoğunluğu artacaktır. Bu etki anten kazancı olarak adlandırılır. Bu kazanç yönlendirilmiş enerji akışı sayesinde meydana gelmektedir. Yönlendirilmiş enerji yoğunluğu formülü:

$$S_g = S_u.G \tag{1.2}$$

S_g: yönlendirilmiş enerji yoğunluğu $[W]$
G: anten kazancı

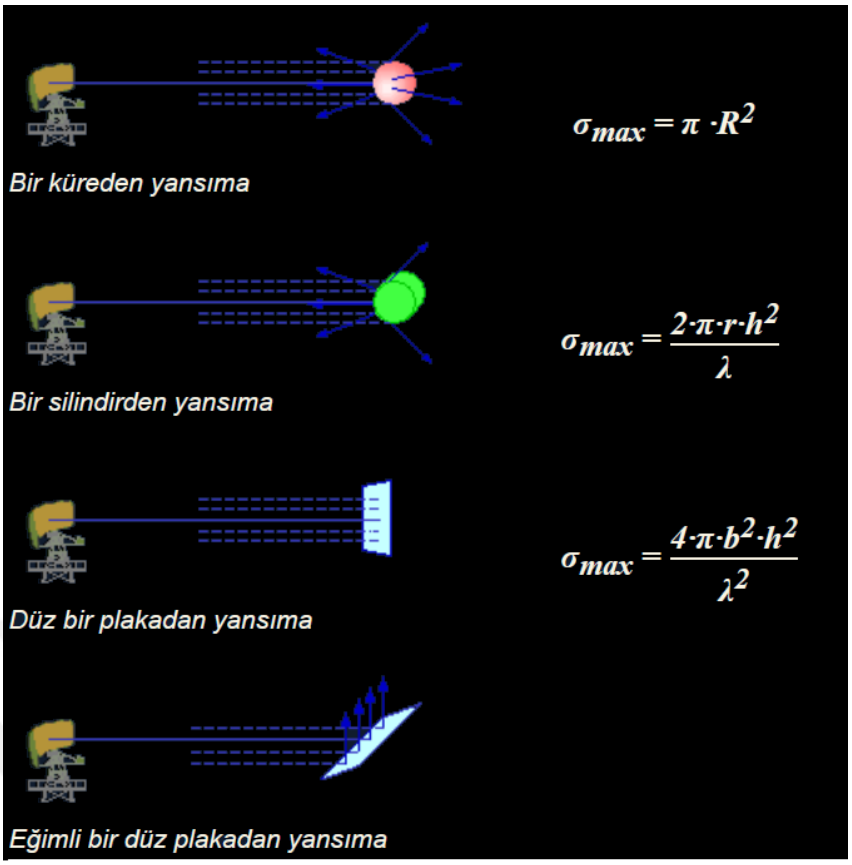
Gerçekte radar antenleri küresel izotropik antenler değil, dar bir demetle dalgalar göndererek yayın yapan 30 dB ya da 40 dB kazanca sahip yönlendirilmiş (örneğin parabolik çanak anten veya faz dizi anten) antenlerdir. Hedefin algılanması sadece hedefin bulunduğu konuma doğru gelen enerji yoğunluğuna değil, aynı zamanda hedefe çarpıp yansıyarak radar anteni yönüne doğru geri dönen enerji miktarına da bağlıdır. Manevra miktarını hesaplayabilmek için radar kesiti ϕ'nin bilinmesi gerekir. Daha büyük yüzey, daha fazla enerjiyi geriye yansıtmaktadır. Yani, Bir Airbus uçağı aynı uçuş şartlarında bir sportif amaçlı kullanılan özel uçaktan daha fazla enerji yansıtır. Bunun yanında, geri yansımanın kalitesi hedefin biçimine, niteliklerine ve hedefte kullanılan malzemeye de bağlıdır. S_u güç yoğunluğunda bir enerjiden hedeften geriye yansıyan güç P_r, anten kazancı G ve radar kesiti ϕ ise

$$P_r = \frac{P_s}{4.\pi.R^2}.G.\phi \tag{1.3}$$

P_r: geriye yansıyan güç $[W]$
ϕ: radar kesiti

Bir cismin radyo dalgalarının yansıma yaptığı bölgesine *radar kesiti* denir. Radar dalgaları, radyo dalga boyuna ve hedefin şekline bağlı olarak çeşitli şekillerde dağılır. Dalga boyu hedefin boyutundan çok daha kısaysa, dalga bir aynadan yansıma yapar şekilde sıçrar. Dalga boyu hedefin boyutundan çok daha uzunsa, zayıf yansıma yüzünden hedef görünmeyebilir. Kısa radyo dalgaları, eğri ve köşelerden yuvarlak bir cam parçasının ışıltısına benzer şekilde yansır. Kısa dalga boyları için en güçlü yansıtıcı hedefler, yansıyan yüzeyler arasında 90 derece açıya sahiptir. Bir köşe reflektörü, bir kutunun iç köşesi gibidir ve algılaması zor nesneleri algılamayı kolaylaştırmak için radar reflektörleri olarak kullanılırlar.

Örneğin, teknelerde bulunan köşe reflektörleri, çarpışmayı önleme ya da kaza sonrası kurtarma sırasında daha algılanabilir hale getirir. Bu önlemler özellikle daha uzun dalga boylarında kırınım nedeniyle yansımayı tamamen ortadan kaldırmaz.



Şekil 1.5 : Radar yansıma çeşitleri.

1.3 Tarihçe

Radar, iniş halindeki uçaklara yardımcı olmak maksadıyla II. Dünya savaşından sonra kullanmaya başlamıştır. Hava trafik kontrolörleri kötü hava şartlarında, uçaklara yol gösteriyordu. Ancak hava sahasında birbirine benzeyen birçok hedef sebep olduğu karışıklık ve takibin zorlaşmasıyla sonucunda uçakları daha kolay tanımlama ve uçuş seviyelerini görebilme imkanları geliştirilmiştir.

Hava sahası gözetimi, seyrüsefer ve haberleşme için kullanılan radarlar, Gösterge İniş Sistemi (ILS), Çok Yönlü Radyo Aralığı / Mesafe Ölçüm Cihazları (VOR/DME) gibi konvansiyonel hava seyrüsefer sistemleri yer temelli sistemlerdir. Bununla birlikte, bu sistemler doğruluk sınırları, aralık ve görüş hatası sınırlamaları, kritik olan birçok kurulum için gereksinimi ve satın alım ve bakım için gerekli olan önemli masraflar gibi birtakım dezavantaja sahiptir. Donanım ve yazılım alanında önemli ilerlemeler kaydedilmesine rağmen, kullanılan teknoloji ilkesi yöntem olarak 40 yılın üzerindedir. Bu sistemler havaalanlarında artan trafik taleplerini karşılamak için daha

Şekil 1.6 : 2. Dünya Savaşı'nda kullanılan Giant Würzburg Radar

fazla geliştirilememekte ve engebeli arazilerden dolayı dünyanın büyük bölümlerine uygulanması zor olmaktadır.

1983 yılında Uluslararası Sivil Havacılık Örgütü (ICAO), uydu navigasyonu alanındaki yeni kavram ve teknolojileri özel bir komiteyi incelemek ve değerlendirmekle görevlendirildi. Geleceğin Hava Seyrüsefer Sistemleri (FANS) Komitesi, dünyadaki havacılık uzmanlarını bir araya getirdi. Böyle bir küresel forumda, bu uzmanlar, havacılık camiasının sonraki bin yılının ihtiyaçlarını en iyi şekilde karşılayacak sistemin planı geliştirilmiştir. İletişim, Seyrüsefer ve Gözetleme / Hava Trafik Yönetimi (CNS/ATM) sistemi olarak bilinen FANS konsepti, var olan mevcut sınırlamaların üstesinden gelmek için, uydulara bağımlı, karmaşık ve birbiriyle ilişkili bir dizi teknolojiyi içerir [9].

1.4 Hava Trafik Yönetimi

ATM, hava trafik hizmetleri, hava trafiği akış yönetimi ve hava sahası yönetimi içeren geniş anlamda tanımlanmış bir işlevdir. Amacı, uçakları birbirinden ayrı tutmak ve uçağın operatörlerinin tercih edilen uçuşa bağlı kalmalarını sağlamak için planlanan varış zamanlarını karşılamalarını sağlamaktır [10]. ATM'ye yeni CNS teknolojilerinin entegrasyonuyla, ATS sağlayıcılarının verimliliği arttırılmaktadır. Uçağın tercih ettiği

uçuş profilindeki minimum ayrımı azaltmak için hava aracı operatörleri ve servis sağlayıcıları, ek hava sahasını serbest bırakmakta, kapasiteyi artırmakta ve aynı zamanda düşük işletme maliyetleri ve gecikmeleri minimuma indirebilmektedir. Şekil 1.7, yeni CNS sistemlerinin ATM'ye olan faydalarını özetlemektedir.

1.5 Hava Trafik Kontrolünde Haberleşme, Navigasyon ve Gözetim

Şekil 1.7 : CNS ATM Faydaları.

ICAO CNS/ATM'yi, "kesintisiz bir küresel hava trafiği yönetim sistemini desteklemek için uygulanan uydu sistemleri ve çeşitli otomasyon seviyeleri ile birlikte dijital teknolojileri kullanan iletişim, seyrüsefer ve gözetim sistemleri" olarak tanımlamıştır [11]. CNS/ATM'nin amacı hava trafik emniyetinin, verimliliğinin ve düzenliliğinin iyileştirilmesi ile hava yolculuğu talebindeki büyümeyi karşılamak için Hava Trafik Hizmetlerinin sağlanmasını desteklemek, kapsamlı ve birleşik bir sistem geliştirmek, hava sahası kullanıcıları ve farklı bölgelerdeki ekipmanları verimli kullanmaktadır. CNS/ATM, insan üzerindeki bağımlılığı azaltarak insan kaynaklı hataları ortadan kaldıran ve hava sahasını optimize etmek için mevcut kısıtlamaları gideren yüksek bir otomasyon seviyesiyle desteklenmektedir. CNS/ATM'nin farklı özellikleri şunlardır:

- *Uydu ile yeryüzüne dayalı sistemlerin karışımı;* Denetleyicilere ve pilotlara tam bir durumsal farkındalık sağlamak için teknik sitelerden operasyonel ünitelere iletişim, navigasyon ve gözetim sistemlerinin veri aktarımı için internetworking sağlar.

- *Küresel kapsam:* Coğrafi yapı engellerine rağmen eksiksiz ATC servislerini mümkün kılar.
- *Güvenilir:* Böylece güvenliğini sağlamak için sürekli ve güvenilir hizmetler mevcuttur.
- *Birlikte çalışabilir sistemler:* Böylece sistem kesintisiz hizmet sunmak için yedekli mimari olarak tasarlanmıştır.
- *Hava-yer veri bağlantısı kullanımı:* Denetleyicilere ve pilotlara senkronize durumsal farkındalık sağlar.
- *Dijital teknolojilerin kullanımı:* Gürültü kesintisi ve yeni dijital uygulama sistemlerine uyum gibi analog teknolojilerin sınırlamalarını hafifletir.
- *Otomasyon seviyesi:* Kontrolörlerin ve pilotların çeşitli işlevlerini yerine getirmelerine yardımcı olmak için daha fazla bilgisayar uygulaması kullanılır.

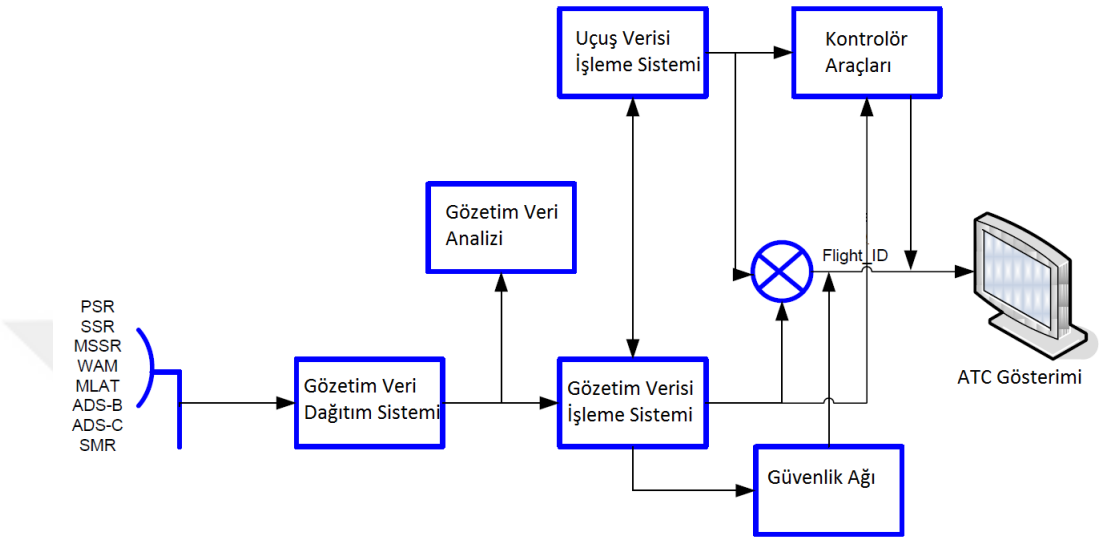
1.6 Gözetim Sistemleri

Uçakları izlemek için kullanılan yöntemlere hitaben gözetim, CNS / ATM'nin üçüncü unsurudur. Sensör, ekran sistemi ve operasyon prosedürlerini içeren gözetim fonksiyonu, hava tahliye kontrolörlerine hava sahasını etkin bir şekilde yönetmek için hava araçlarının güncel pozisyonu sağlamaktadır. Sürveyans sensörünün türüne bağlı olarak uçak tanıma ve hız gibi ek bilgiler de sunulmaktadır. Ayrıca gözetim fonksiyonu, yörünge tahmini ve durumsal farkındalık gibi bir dizi uygulamaları da desteklemektedir.

ATC Gözetim sistemi Şekil 1.8'de gösterilmektedir. Şekil 1.8'deki ana bileşenler şunlardır:

- *Gözetim Veri Dağıtım Sistemi:* Verileri standart bir formata (ör. ASTERIX) dönüştürür ve daha sonra verileri diğer cihazlara iletir.
- *Gözetim Veri İşleme Sistemi:* İz durum vektörünü oluşturmak için çizimleri tahmin eder.
- *Gözetim Veri Analizi Aracı:* Veri performansını analiz eder.

- *Güvenlik Ağı:* Tehlikeli durumların büyük olaylara ya da kazalara dönüşmesini önlemek için kullanılır.
- *Uçuş Veri İşleme Sistemi:* Uçuş planını depolar, görüntüler ve günceller.



Şekil 1.8 : ATC gözetim sistemi

ATC gözetim sistemi için şartlar kullanılan uygulamalara bağlıdır. Bununla birlikte, tek bir gözetim sistemi hava trafiği terminal alanlarına kadar değişen trafik koşullarına sahip her hava sahasındaki tüm uçuş fazları için sürveyans gerekliliklerini karşılayabilir. Kullanılan mevcut gözetim sistemleri aşağıdaki gibidir;

- Birincil Gözetim Radarı (PSR)
- İkincil Gözetim Radarı (SSR)
- Monopulse İkincil Gözetim Radarı (MSSR)
- Yüzey Hareketi Radarı (SMR)
- Çok Taraflı Gözetim (MLAT)

Bu teknolojiler sonraki bölümlerde ayrıntılı olarak açıklanmaktadır. Sürveyans sistemlerinin kategorizasyonu Çizelge 1.1'de ve gözetim sensörleri performans karakteristikleri Çizelge 1.2'de gösterilmektedir. Son zamanlarda, Otomatik Bağımlı Gözetim (ADS) adı verilen yeni bir sürveyans teknolojisi ortaya çıkmıştır. Gelecekteki

Çizelge 1.1 : Gözetim Sistemleri Kategorizasyonu

Gözetim Kategorisi	Gözetim Radarı Teknolojisi
İşbirliği Gerektirmeyen İşbirliği Gerektiren Bağımsız İşbirliği Gerektiren Bağımlı	- Birincil Gözetim Radarı (PSR) - İkincil Gözetim Radarı (SSR) Mode A/C - İkincil Gözetim Radarı (SSR) Mode S - Otomatik Bağımlı Gözetim Sistemi (ADS-B)

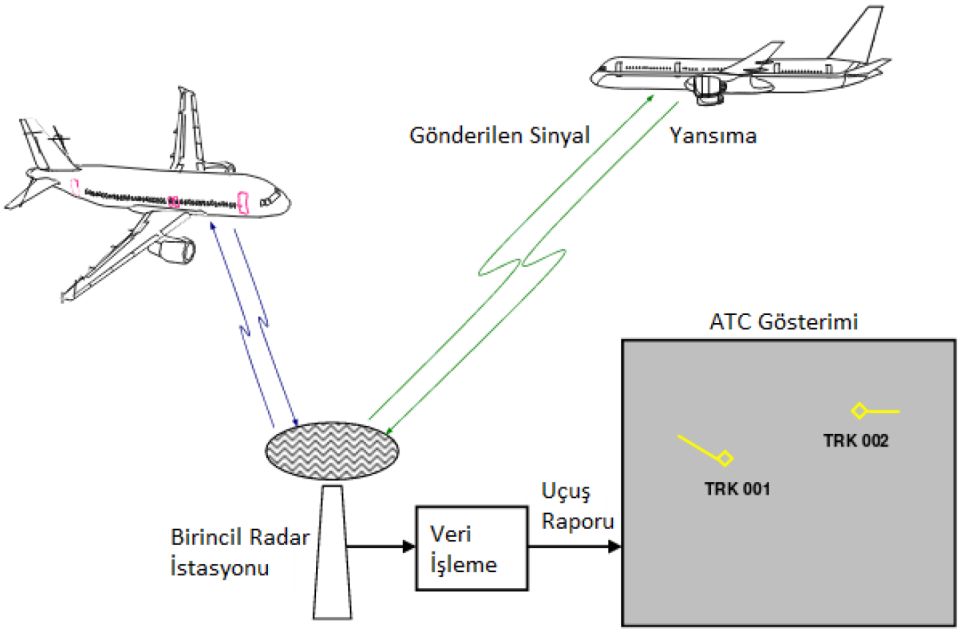
Çizelge 1.2 : Gözetim Sensörleri Performans Karakteristikleri

Gözetim Sistemleri	Kapsama [NM]	Doğruluk	Bütünlük	Güncelleme [sn]
Birincil Gözetim Radarı (PSR)	S-Bant: 60-80 L-Bant: 160-220	Menzil: 0.1 NM Azimut: 0.15 deg.	Bütünlük raporu iletilmez.	4-15
İkincil Gözetim Radarı (SSR) Mode A/C	200-250	Menzil: 0.03 NM Azimut: 0.07 deg	Bütünlük raporu iletilmez.	4-15
İkincil Gözetim Radarı (SSR) Mode S	200-250	Menzil: 0.03 NM Azimut: 0.07 deg	Bütünlük raporu iletilmez.	4-12
ADS-B	200-250	GPS: <0.1 NM	Pozisyon bütünlüğü ADS-B mesajıyla gönderilir.	0.5-2

hava trafiği yönetimini karşılamak için birçok yeni gözetleme uygulamasını desteklemektedir. ADS, navigasyon ve iletişim işlevlerini kullanmaktadır. Farklı gözetim teknolojilerinin bulunması, gerekli operasyonlara en uygun ve etkili gözetim sistemini seçme esnekliği sağlar. Bununla birlikte, gözetim işlevinin uyumluluğunu sağlamak için, tüm işletim gereksinimleri sürveyans teknolojisi göz önüne alınmaksızın bir dizi gözetim performans parametresine dönüştürülmektedir.

1.6.1 Birincil Gözetim Radarı (PSR)

Hem sivil hem askeri radarların temelini oluşturur. Birincil Gözetim Radarı (PSR), Şekil 1.9'da görüldüğü gibi yer istasyonundaki kendi ekseni etrafında 360 derecelik dönüş yapabilen bir anten yardımı ile elektromanyetik radyo dalgaları gönderen bir sistemdir. Radyo dalgaları karşılaştıkları bir hedeften yansıması sonucu antendeki alıcı tarafından işlenir. Eğer hedef hareket ediyorsa anten her dönüşte hedefin pozisyonunu yeniler ve bu şekilde hedefin yönü belirlenmektedir.

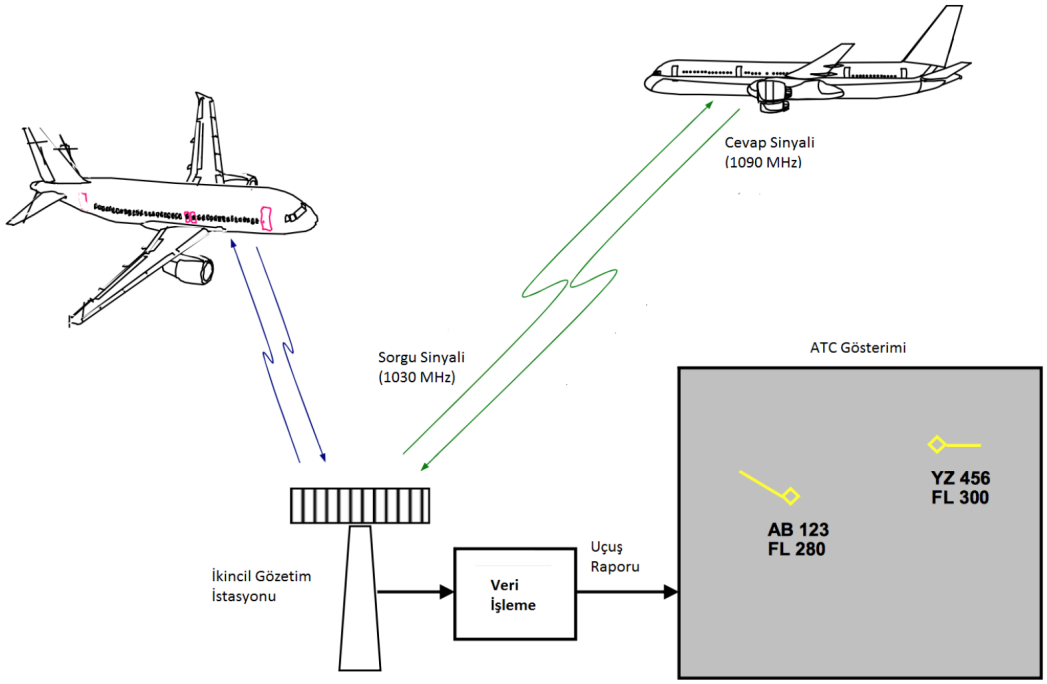


Şekil 1.9 : PSR Şeması.

PSR ilgili trafiğin sadece iki boyutlu pozisyonu verebilir, irtifa bilgisi vermez. Hava aracının etrafındaki diğer hava araçlarının yansımaları nedeniyle ilgili hedefi tanımlamada birtakım güçlüklerle karşılaşılır. Dolayısıyla PSR görüntülediği hedefler arasında ayrım yapamamaktadır. Kontrolör çoğu zaman ilgili hava aracını tanımlayabilmek için rota değişiklikleri yaptırmak zorunda kalır. Radar ekranında gözlemlenen hedeflerden yaklaşık yarısı tanımlanmamış trafiklerdir. Radyo temasının olduğu bütün pilotlardan irtifa, sürat gibi hava trafik kontrolü ile ilgili bilgileri sık sık talep etmek gerekmektedir [12].

1.6.2 İkincil Gözetim Radarı

İkincil Gözetim Radarı (SSR) ile hava araçlarından üç boyutlu bilgi alınabilmektedir. Hava ve yer cihazları arasında koordinasyon bulunmaktadır. Yer istasyonunda sorgulayıcı, hava aracında bulunan cihaza da cevaplayıcı denir. Yer istasyonundaki sorgulayıcıdan uçaktaki göndericiye bir sorgulama sinyali gönderilir ve bu sinyal özel bir kodla tekrar gönderici tarafından tetiklenerek yeniden radara yollanır ve sinyal işlendikten sonra radar ekranında görüntülenir [13]. SSR şeması Şekil 1.10'da sunulmuştur.



Şekil 1.10 : SSR Şeması.

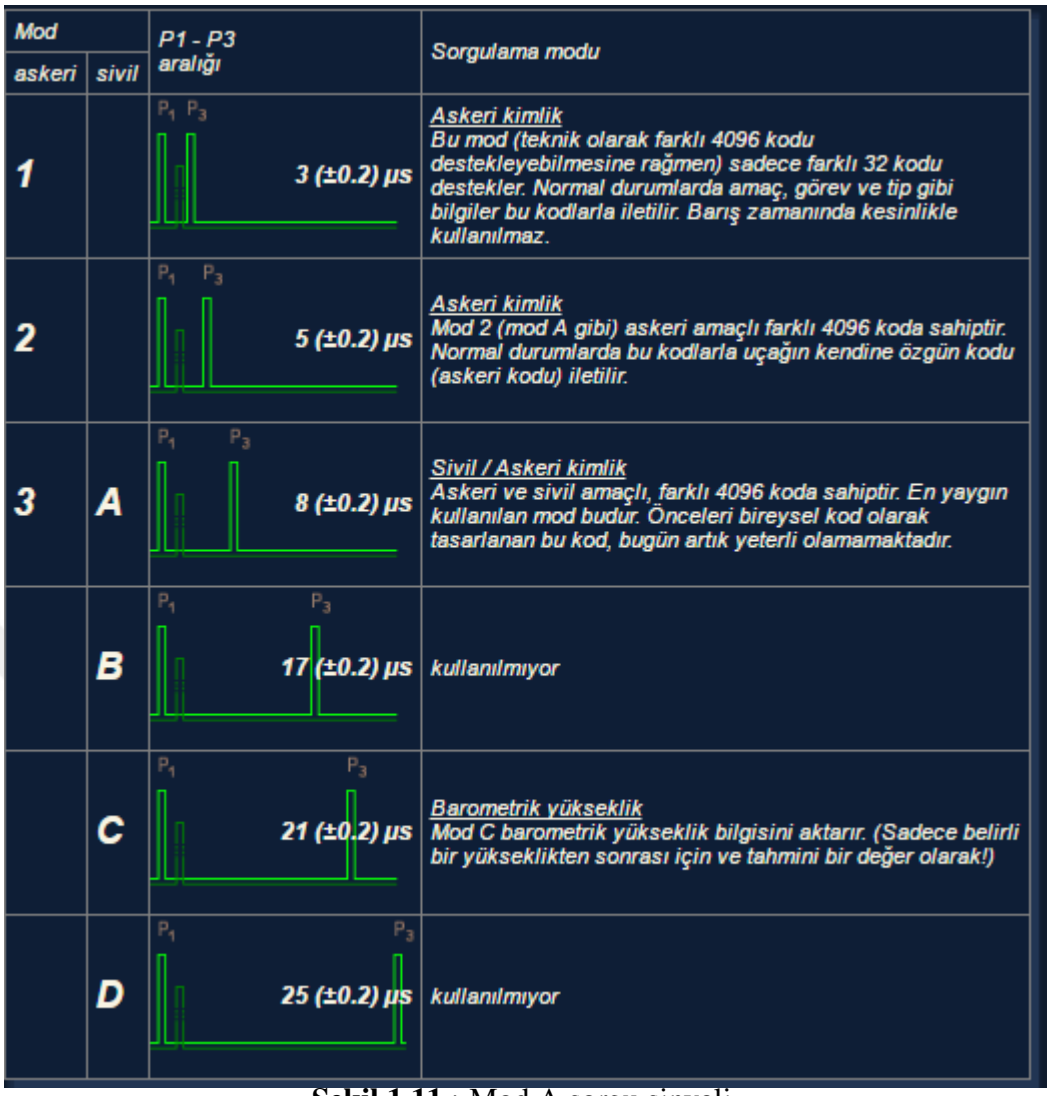
Hava araçlarının birbirine mesafe ve yön olarak çok yakın olduğu konumlarda, SSR cevaplamaları birbirlerinin üzerine binmekte, yer istasyonu bu cevaplamaları çözümleyememekte ancak bilgiyi kaydetmektedir. Hava araçlarının etrafında bulunan birçok SSR istasyonu nedeniyle, bir tanesi için gönderilen yanıt sinyali, başka bir istasyon tarafından alınmakta ve işlenmektedir ancak bu istasyonlar hava aracını yanlış pozisyonda göstermektedir [12].

1.6.2.1 Mod A

Mod A sorgulama, uçağın transponderinden gelen, bireysel uçak tanımlama sağlayan mesaj üretir ve bu tanımlama hava trafik kontrolörü tarafından operasyonel amaçlar için kullanılmaktadır [14].

İkincil radarların sorgulama formatı Uplink-format olarak adlandırılır. Uplink, yer-uydu arası bağlantı anlamına gelir. Sorgulamada birbirleri arasında 0,8 μs lik zaman aralığı bulunan iki adet darbe (P1 ve P3) kullanılır. Şekil 1.11'de belirtilen sorgulama modunda aralıklardan bahsedilmiştir.

Yanıt telegramı, herbirinin darbe genişliği 0,45 μs (-+0,1 μs) olan, 2 ila 15 darbeden meydana gelir. Bu iletinin geçerli sayılması için aralarında 20,3 μs zaman aralığı bulunan her iki çerçeve darbesi F1 ve F2 in varlığı şarttır. Bu iki çerçeve darbesi

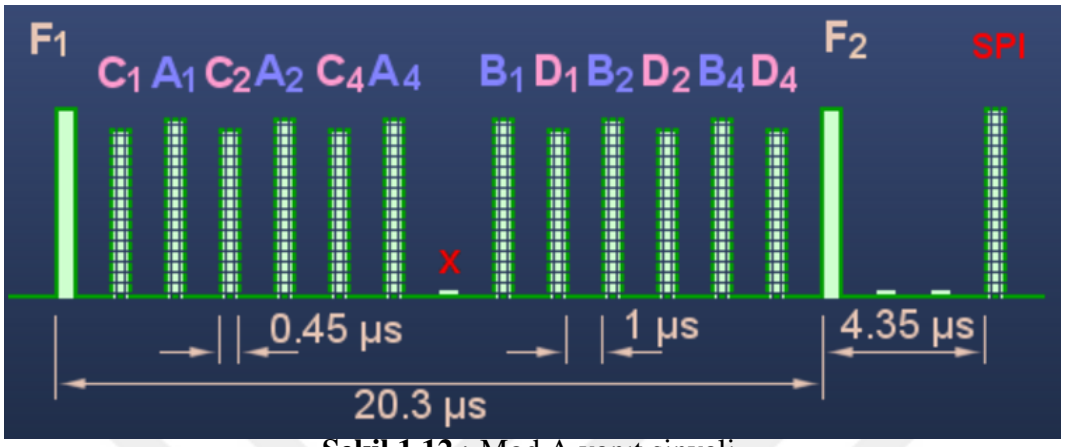


Şekil 1.11 : Mod A sorgu sinyali.

arasında 1,45 μs de tekrarlanan, 13 adet kodlama darbesi bulunur. Bir oktal (sekiz tabanlı) kod ile Mod A ve Mod C de bu darbelerden en fazla 12 adedi istenen bilgilerin iletilmesi için kullanılır. Boşta kalan üç yerde bir darbe kullanılmaz, aksi takdirde bazı dekoderler toplam iletiyi parazit olarak değerlendirebilir ve bunun sonucu olarak iletiyi reddedebilirler.

Yanıt telegramı hiç bir şekilde modun ne olduğu hakkında bilgi içermez. İkincil radarın yanıt çözücüsü alınan yanıt telegramının kodunun, daima en son alınmış telegramın moduyla aynı olduğunu kabul etmektedir. Çerçeve darbeleri arasında bulunan darbeler, istenen bilgileri oktal sayı ile tutan sorgulama moduna bağımlıdır. Şekil 1.12'de görüldüğü gibi mümkün olan 12 adet darbe ile birbirinden farklı en fazla 409610 veri kodlanabilir [14].

Mod A kullanılması durumunda uçağın kontrol panelindeki transpondere oktal kod $(ABCD)_8$ yüklenir. C modunun kullanılması durumunda uçuş yüksekliği Gillham kodu (yükseklikte değişmelerinde sadece bir bitin değiştiği Gray kodunun özel bir biçimi) adı verilen bir kod ile iletilir.



Şekil 1.12 : Mod A yanıt sinyali.

Uçuş güvenliğinin gerektirdiği durumlarda yanıt özellikle vurgulanır ve bir SPI darbesi (Special Purpose Identification - Özel Amaçlı Kimlik) kullanılır. Yer istasyonu personelinin isteği üzerine pilot kontrol panelindeki bir düğmeye basar ve yanıt telegramına belirli bir süre için (18+-1 μs kadar) SPI darbesi eklenerek birlikte yollanır. ICAO ya uygun olarak bir SPI darbesi sadece A modunda yaratılabilir [14].

1.6.2.2 Mod C

Mod C sorgulaması, uçak transponderinden kodlanmış basınç yüksekliğini ifade eden mesajı üretir. Mod C sorgulaması barometrik yükseklik sorgusu olarak da bilinir. Basınç yüksekliği hava sahasında dikey ayrılmayı ifade etmektedir [14].

1.6.2.3 Mod S

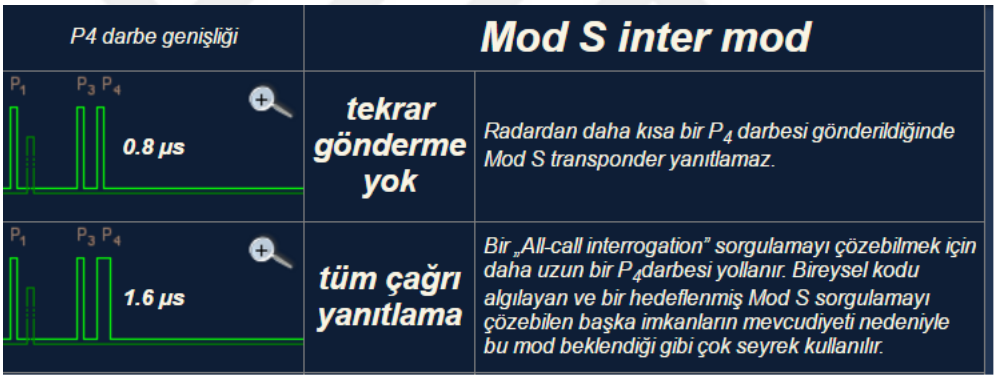
Mod S ve Mod A/C uçakları ve zemin öğeleri arasındaki operasyonel uyumluluk, protokollerin kullanımı ile sağlanır. Modlar arası işlemler, Mod S yer istasyonlarının ilgili uçakları belirlemek için, Mod S ve Mod A/C transponderlerini eşzamanlı olarak sorgulamasına izin verir. Intermod sorgulamaları ayrıca, yer istasyonunun yalnızca Mode A/C veya Mode S cevaplarını almasına izin verir, ancak eş zamanlı olarak cevaplamaz [14].

Daha eski ikincil radarlarda tipik sorgulama formatı Mod C idi. Bu formatı daha sonra Mod C ve diğer modlar takip etmiştir. Modlardaki bu değişim, yayın alanı

içinde bulunan bütün uçakların algılanabilirliğini garanti edebilmek için sürekli hale gelmiştir. Mod S sorgulama yapabilen bir yer istasyonu çok değişik tür sorgulama yapabilme imkanına sahiptir. Bunları kabaca iki ayrı sınıfta toplayabiliriz [14]:

- *Tüm çağrı sorgulama (All-call interrogations):* Algılama bölgesinde ki bütün uçaklardan bir yanıt bekler. Fakat bazı belirli durumlarda Mod S transponder yanıt vermeyebilir.
- *Tek çağrı sorgulama (Roll-call interrogations):* Sadece sorgulanan transponder yanıtlar.

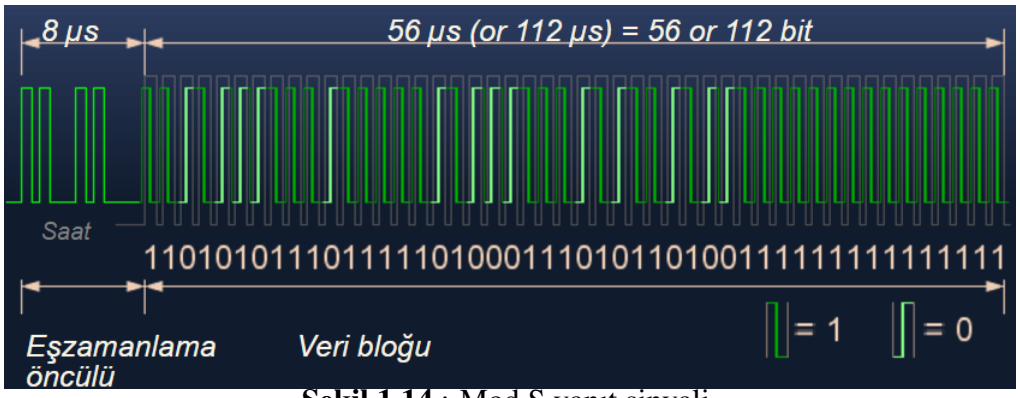
Mod S sistemi için ilk iş bireysel sorgulama yapabilmek için algılama bölgesinde bulunan uçakların bireysel adreslerini ortaya çıkartmaktır. Bu işlem ikincil radardan periyodik olarak yollanan tüm çağrı sorgulamada kullanılmaktadır. Mod S sorgulama çeşitleri Şekil 1.13'te detaylandırılmıştır.



Şekil 1.13 : Mod S sorgu sinyali.

Şekil 1.14'te görüldüğü gibi Mod S yanıt telegramı iki kısımdan meydana gelir:

- *Eşzamanlama öncülü:* Her Mod S yanıtı 8 μs lik bir eşzamanlama öncülü ile başlar. Darbe deseni her biri 0,5 μs süreli 4 adet darbeden meydana gelir. Darbeler arasındaki zaman aralığı ilk darbeye göre 1; 3,5 ve 4,5 μs dir.
- *Veribloğu* Her biri 1 μs süreli 56 ya da 112 darbeden meydana gelir, yani toplam 56 veya 112 bittir. Daha kısa olan 56 μs lik yanıtta kimlik tanıma için 5–bitlik veri blok format numarası, 27–bitlik bir gözetim bilgisi veya kontrol bloğu bulunur ve keza bir eşlik bilgisini de içeren, uçağa ait 24-bitlik bir bireysel kod numarası ile sonlanır.



Şekil 1.14 : Mod S yanıt sinyali.

1.6.3 Eşzamanlı Olmayan Hatalı Cevaplar

Bir uçan hedefin uçuş rotasında farklı radar algılama bölgelerinden geçmesi nedeniyle aynı taşıyıcı frekansları kullanılması gerekmektedir. Radar ağlarının göreli yoğunluğu ve artan hava trafiği nedeniyle birçok uçan hedef farklı radar istasyonları tarafından sorgulanmakta ve bu sorguların karşılığı olarak yanıtlar uçan hedef tarafından radar istasyonuna gönderilmektedir. Böylece radar istasyonlarına artan hava trafiği nedeniyle parazit gelme olasılığı daha da fazladır. Özgün sorgulama sinyali içinde çözülemeyen, yanıtların sebep olduğu bu parazitlerin tümüne FRUIT adı verilir. Sonuçta bu sayının azaltılması ve optimizasyonu için önlemler alınmıştır. Bu önlemler arasında [15]:

- Yerde veri hatlarını kullanarak veri iletişimi yapan sorgulama istasyonu sayısını azaltmak,
- Gönderim gücünü makul bir seviyeye düşürmek,
- Darbe Tekrarlama Frekansını (PRF) mümkün olduğunca küçük seçmek,
- Sadece gerektiğinde sorgulama yapmak,
- Sektörsel sorgulama,
- Hedef denetlemeli sorgulama,
- Yan Lob Bastırma yönteminin optimizasyonu,

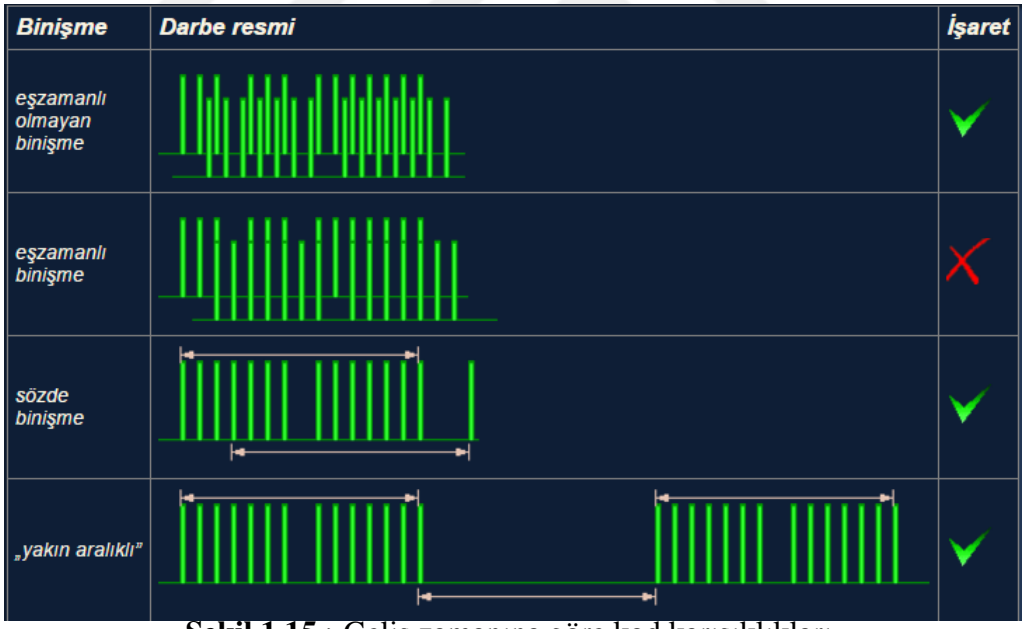
bulunmaktadır. Mevcut parazitlerinin optimizasyonu için alınan bu önlemlerde yeterli olamadığından parazit giderici (defruiter) denilen bir aygıt kullanılır [15].

1.6.4 Kod Karışıklığı

Sinyallerin birbiri üstüne binişerek bozulmasıdır, Bir yanıt telegramının uzunluğu yaklaşık 20,3 μs dir. Bu, sürede bir elektromanyetik dalga 3 km yol alır. Yönlü bir antenin algılama bölgesinde aralarında 3 km radyal açıklık bulunan iki yada daha fazla sayıda uçan hedef yer aldığında bu hedeflerden gelen yanıt telegramları kısmen birbiri ile karışır [16]. Bu olaya binişme veya kod karışıklığı adını verilir. Binişmenin temelde iki türü bulunur:

- Eşzamanlı olmayan binişme
- Eşzamanlı binişme

Şekil 1.15'te görüldüğü gibi tarama zamanları çakışmayan iki yanıt birbiri üstüne bindiği zaman eşzamanlı olmayan binişme dediğimiz binişme meydana gelir. Böyle yanıtlar birbirinden ayrılamamakta ve kodları çözülememektedir [16].



Şekil 1.15 : Geliş zamanına göre kod karışıklıkları.

Eğer tarama zamanları ortak iki sinyal birbiri üstüne binerse *eşzamanlı binişme* meydana gelir. Kod çözülmesi sırasında her bir darbenin hangi yanıta yada her iki yanıtın ikisine de ait olup olmadığını anlamak mümkün değildir. Bu nedenle kod çözülmesi sonucunda bütünüyle yepyeni ve orijinal yanıtla ilgisi olmayan yanıtlar devreye girer. Bilgisayar kontrolüyle veriler işlenirken, bu boşluklar dikkate alınmaz ve ekrana gönderilmez. Fazla sayıda anlamı bulunan veya hatalı yanıtların doğru

olanlardan ayrıştırılma işlemine *Binişme Giderme* adı verilir [16]. *Sözde binişme*, doğru yanıttır ve ekranda da görüntülenmesi gerekmektedir. Özellikle gerekiyorsa, uçağın pilotu ile telsiz görüşmesi yapılır. Ancak bu konuşma sırasında uçak ekranda kaybolabilir. Yanıtlar birbiri üzerine binmediğinde, darbeler 20,3 μs gibi bir yakın aralıkta yer alabilir. Basitçe binişme giderme algoritmaları bu durumu bir binişme olarak algılar ve her iki yanıtın çözülebilmesine rağmen ekrana gitmesini engelenir [16].

2. OTOMATİK BAĞIMLI GÖZETİM - YAYINI

2.1 Yeni Nesil Havacılık Sistemi

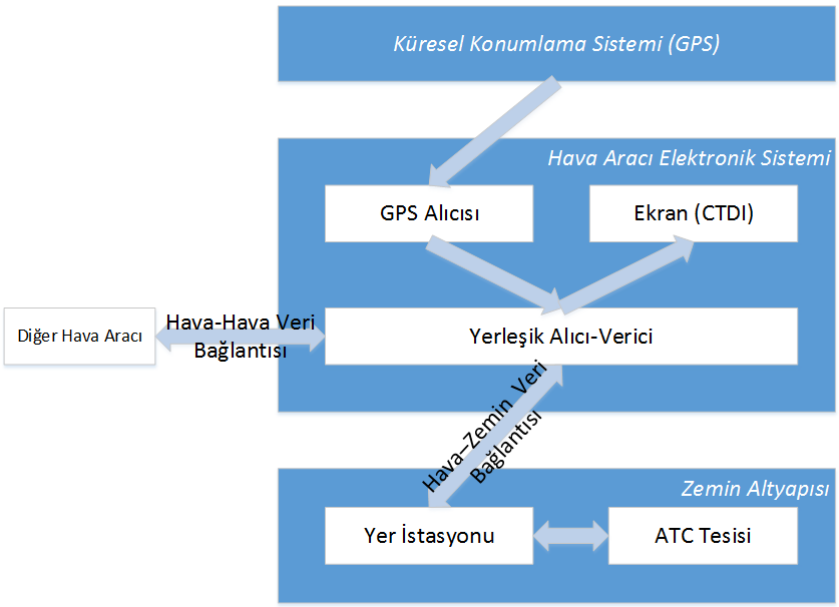
Yeni Nesil Havacılık Sistemi uçakların kısa sürede A noktasından B noktasına doğrudan geçmelerini sağlayan kapsamlı bir teknoloji çözümüdür. Yakıt tüketimini ve çevre üzerindeki etkiyi azaltarak yolcuların zamanında varış noktalarına ulaşmalarına yardımcı olur. Yeni nesil gözetim sistemi NextGen'in aşağıdaki özellikleri sağlaması gereklidir [8]:

- *Temel Gözetim:* Günümüzde kullanılan gözetim sistemlerinden daha iyi performans sergilemelidir. Bunun yanında çok işlevli yetenekleri de etkinleştirmelidir. Hizmetleri maliyeti düşük bir şekilde sunmalıdır.
- *Kokpit Danışma Hizmetleri:* Pilotların durumsal farkındalık ve karar verme yeteneklerini geliştirmek için trafik, hava durumu ve veritabanı yönetim kolaylıkları sağlamalıdır.
- *Kokpit Kritik Hizmetler:* Uçakların daha güvenli bir şekilde uçmasına izin vererek kapasiteyi artıracak gelişmiş kokpit görüntüleme uygulamalarını etkinleştirmelidir.

2.2 Otomatik Bağımlı Gözetim Yayını

ADS-B, günümüzde Hava Trafik Yönetiminde haberleşme–navigasyon–gözetim uygulaması paradigmasını baştan tanımlayan yeni bir teknolojidir [8]. ADS-B, geleneksel radardan çok daha düşük maliyetli olarak kullanılmış ve sertifikalandırılmıştır. Kullanılan ADS-B teknolojisiyle pilotların ve hava trafik kontrolörlerinin uçakları daha hassas bir şekilde takip etme ve kontrol etmesi mümkün olmaktadır.

- **Otomatik:** Her zaman açıktır ve operatör müdahalesi gerektirmez.
- **Bağımlı:** Konum verileri için GNSS sinyaline bağlıdır.
- **Gözetim:** İlkel radar mantığına benzer ancak daha kabiliyetli gözetim hizmetleri sağlar.



Şekil 2.1 : ADS-B Sistem Mimarisi.

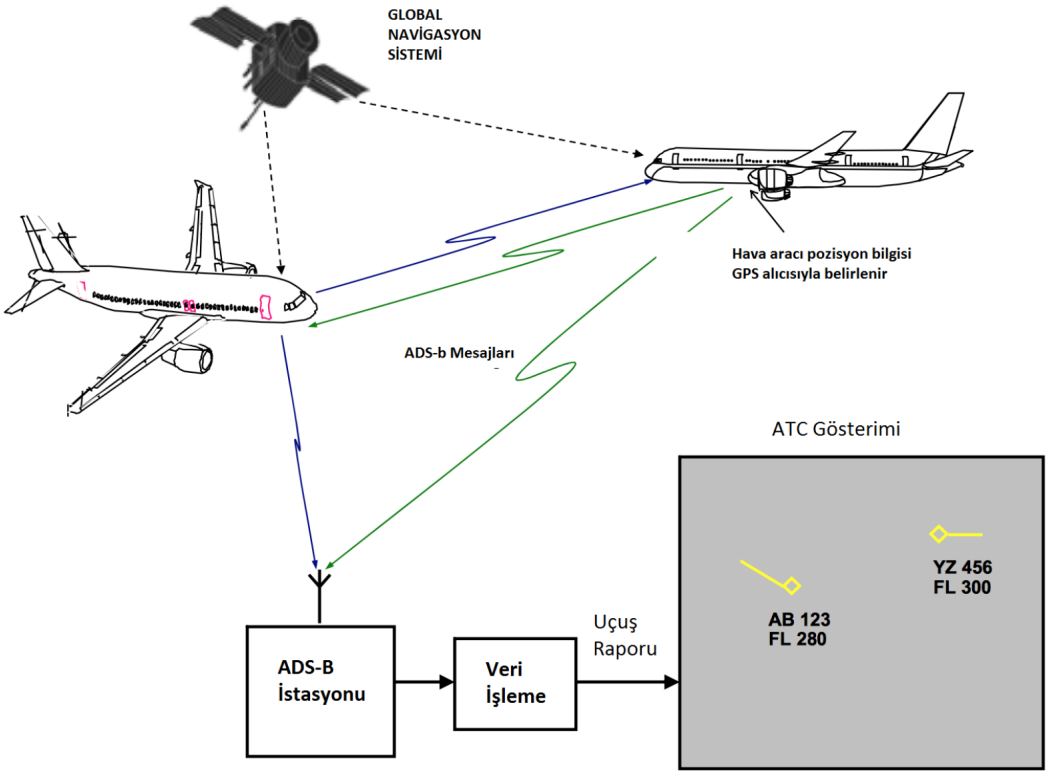
- **Yayın:** Uçak pozisyonunu ve diğer verileri, ADS-B'yi almak için donatılmış bir uçağa veya yer istasyonuna sürekli yayın yapar.

Otomatik Bağımlı Gözetim Yayını gerçek zamanlı pozisyon, hız, kimlik ve uçuş bilgilerini içeren uçak yayınıdır. ADS-B Sistem Mimarisi Şekil 2.1'de gösterilmektedir. Mod S göndericisine sahip uçaklar özel sorgulara ihtiyaç duymadan, bilgileri periyodik aralıklarla otomatik olarak yayınlar. Hava araçları GPS alıcısı vasıtasıyla kendi pozisyonlarını, hava trafik kontrol merkezlerine ve yer istasyonlarına iletir. Alıcılar lokasyon bilgisinin temini açısından uçağa bağımlıdır. Bu yayın herhangi bir sorgulayıcı olmadan saniyede iki defa 1090 MHz frekans bandında DF17 veri formatında iletilmektedir. PSR ve SSR'a göre çok daha ucuz bir maliyeti vardır ve alıcı anteni 10 kiloyu geçmemektedir [6].

ADS-B, güvenlik ve verimliliği artıran ve pilotlara, denetleyicilere, havaalanlarına, havayollarına ve halka doğrudan fayda sağlayan çevre dostu bir teknolojidir ve Şekil 2.2'de görülebilmektedir. Yer radarından ve seyir yardımcılarından uydu sinyalleri kullanıp kesin izlemeye geçerek NextGen'in temelini oluşturur.

ADS-B ile, pilotlar ilk kez denetleyicilerin gördüklerini görüntüleyebilmektedir. Bunlar;

- gökyüzündeki diğer uçakları gösteren görüntüler.
- kokpit görüntüleri,

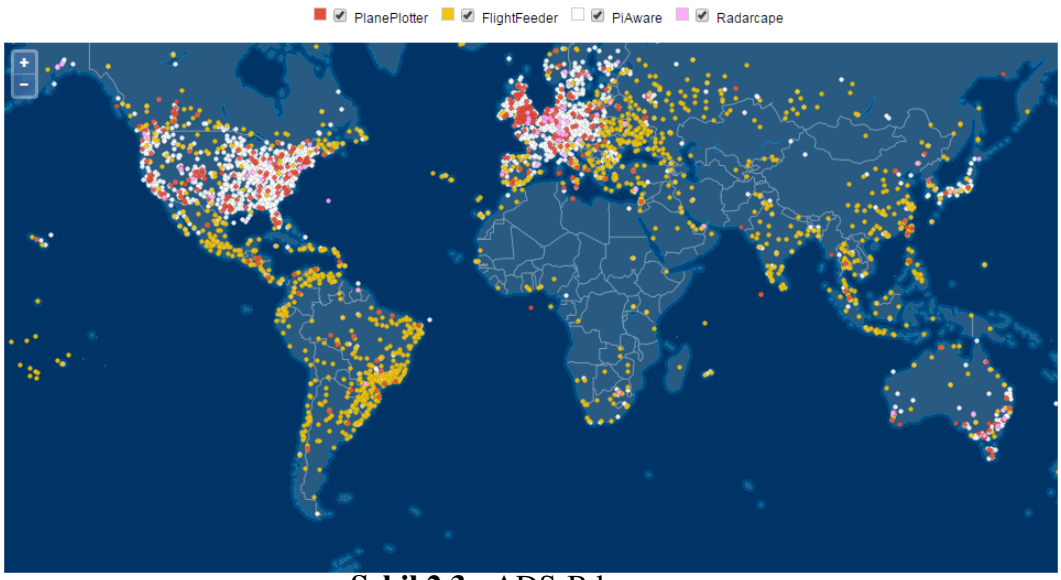


Şekil 2.2 : ADS-B Şeması.

- tehlikeli hava ve arazi görüntüleri,
- geçici uçuş kısıtlamaları gibi önemli uçuş bilgileridir.

ADS-B uygulamaları halen geliştirilmekle birlikte pilotlara potansiyel çarpışma tehlikelerine ilişkin uyarı verme yeteneğine sahip olacaktır. ADS-B'nin en büyük avantajlarından biri, radarın daha önce erişemediği kapsama alanı sağlamasıdır. ADS-B kapsamı Şekil 2.3'te oku Kapsama alanının artmasıyla okyanuslararası ulaşımlar daha etkin takip edilebilmektdir. Stratejik olarak yerleştirilmiş yayın istasyonları, yakınlardaki sinyalleri alıp onları yönlendirilmiş aralıktaki herhangi bir alıcıya yayınlama olanağı sağlar. Bu nedenle, ATC tesislerinin dikkatle yerleştirilmesiyle, hava aracı çevrelerindeki hareketliliği hassas bir şekilde algılayacak ve böylece daha fazla doğruluk, çözünürlük, bütünlük ve güvenlik sağlayacaktır [6].

Denetleyiciler, uçaklar arasındaki minimum takip mesafesini güvenli bir şekilde azaltabilir ve hava trafiği kapasitesini artırabilir. Konum belirlemede yerdeki ilkel radarlar yerine uydulara dayanmak, uçakların A noktasından B noktasına doğrudan uçması, zamandan ve paradan tasarruf edebilmesi, yakıt ve emisyonların azaltılması anlamına gelmektedir.



Şekil 2.3 : ADS-B kapsamı.

ADS-B kabiliyetli uçaklar, kesin konumunu çıkarmak için sıradan bir GNSS (GPS, Galileo vb.) alıcısı kullanır ve bu konumu, hız ve yükseklik bilgileri uçuş numarası gibi hava aracı tanım bilgisi ile birleştirir. Bu bilgi aynı anda diğer ADS-B özellikli uçaklara ve ADS-B alıcılarına yayınlanır. Bu sayede uçak pozisyonunu ve ek bilgiyi Hava Trafik Kontrol merkezlerine gerçek zamanlı olarak aktarır.

GPS alıcısı için risk, konum ölçümü tespitinin ne kadar hatalı olabileceğidir. Konum hatası yeterince büyük olursa, hava trafik kontrolü, hava trafiğinde güvenli bir ayrım sağlayamamaktadır. Sertifikalı GPS sensörleri, GPS uydu ölçümleriyle karşılaştırır. Bir uydu sinyali hatası algılanacak kadar büyük olduğunda, alıcı bu sinyali reddedecektir. ADS-B kuralında belirtilen bütünlük performansı, bu hata algılama algoritmalarının düzgün çalışmasına bağlıdır. GPS ölçümlerine dayalı olarak ADS-B konumlandırma güvenliğini sağlanır [8] .

Sertifikandırılmamış ticari amaçlı GPS sensörleri uydu ölçümlerinde hataları tespit etme algoritmalarını barındırmayabilir. Konum verileri hatalı bir ölçümle sunulduğunda güvensiz bir durum sözkonusu olmaktadır. Bu nedenle, bu sertifikalandırılmamış sensörlere dayalı ADS-B konumu, hava trafiği ayırma ve ADS-B hava-hava operasyonlarını desteklemek için kullanımı yasaklanmıştır.

Son olarak, ADS-B, Trafik Çarpışma Kaçınma Sistemini (TCAS) uygulayacak potansiyele sahiptir. TCAS sistemlere havadan çarpışmayı önleme yeteneklerini arttırma olanağı tanır. TCAS, uçakları (SSR'ye benzer şekilde) sorguya çekerek ve

Çizelge 2.1 : ADS-B mesaj içeriği

DF 5	** 3	ICAO 24	DATA 56	PI 24

Çizelge 2.2 : ADS-B mesaj içeriği açıklamaları

Bit Sayısı	Bitler	Kısaltma	Açıklama
5	1-5	DF	Downlink formatı
3	6-8	CA	Kabiliyet
24	9-32	ICAO	ICAO hava aracı adresi
56	33-37 33-88	[TC] DATA	Veri
24	89-112	PI	Parite/Sorgulayıcı ID

sorguları yanıtlayarak izlemeye çalışır. Daha sonra, TCAS, bir uçağın başka bir hava aracının güvenlik bölgesi içine girip girmediğini belirler. Bir uçak bu bölgeye girdiyse, uçağa bir trafik danışmanı gönderilir. Uçak gerekli düzeltmeyi yapmazsa, çarpışmayı önlemek için bir çözüm önerisi (dikey manevra komutu) iletilir [17]. ADS-B sadece hava ile çarpışmayı önlemekle kalmaz, uçak yerdeyken ADS-B mesajlarını iletmeye devam eder. Bu, pistten kaçınma ve apron yönetimi için yüzey gözetimi sağlar. ADS-B'nin pek çok avantaj mevcut olsa da, tüm yeni teknolojiler gibi, dezavantajlar ve zayıf noktaları da vardır.

2.3 ADS-B Mesajı

Bu bölümde ADS-B sinyalinin içerdiği bilgilerden bahsedilmektedir. Bir ADS-B mesajı 112 bit uzunluğundadır ve 5 parçadan oluşur.

Herhangi bir ADS-B mesajı, ilk 5 biti 10001 ile başlamalıdır. 6-8 arası bitler, ADS-B mesajının farklı tipleri içinde farklı anlamlara sahip tanımlamalar kullanılır [18].

Bir ADS-B mesajında hangi bilgilerin bulunduğunu belirlemek için ADS-B mesajının 33-37 bitleri arasında belirtilen mesajın Tip Koduna bakılması gerekir [18]. Aşağıda, her Tip Kodu ve veri bölümünde yer alan bilgiler ve arasındaki ilişki verilmiştir.

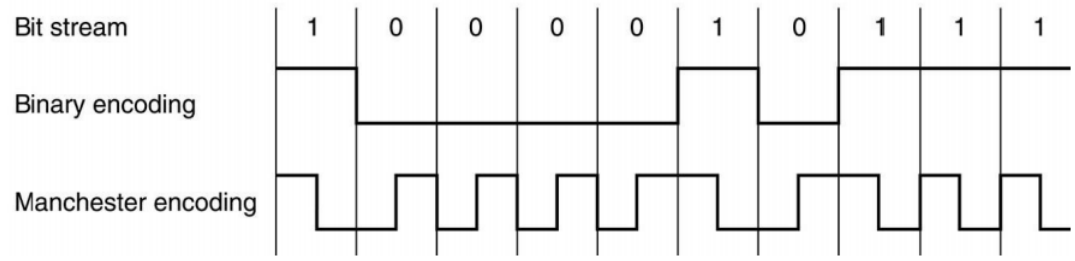
Çizelge 2.3 : ADS-B mesajı örneği

HEX	8D	4840D6	202CC371C32CE0	576098
BIN	1001 101	010010000100 000011010110	[00100]0000010110011000011011 10001110000110010110011100000	010101110110 000010011000
	DF CA	ICAO	[TC] DATA	PI

Çizelge 2.4 : ADS-B mesajı çeşitleri

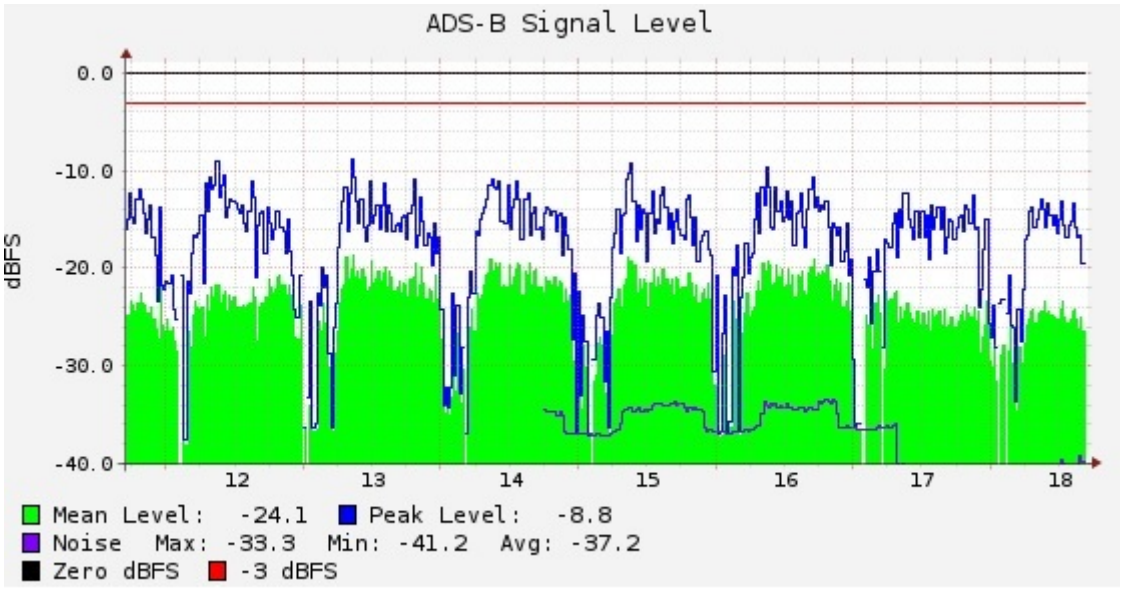
TC	İçerik
1-4	Hava aracı kimliği
5-8	Yüzey pozisyonu
9-18	İrtifa (GPS)
19	Hız (GPS)
20-22	Pozisyon (GPS)
23-31	Diğer kullanımlar

ADS-B mesajını kodlamak ve iletmek için Darbe Konum Modülasyonu (PPM) kullanılır. PPM, verinin içerdiği tüm darbelerin ilk veya ikinci yarısını işgal etmesi anlamına gelir bu da Şekil 2.4'te görüldüğü gibi Manchester kodlamasına eşdeğerdir.



Şekil 2.4 : ADS-B Manchester kodlama.

Tüm bu özellikler sonucunda yer alıcısından toplanan gerçek bir ADS-B mesajı örneği Şekil 2.5'te görüldüğü gibidir.



Şekil 2.5 : ADS-B gerçek sinyal örneği.

3. ADSB'DE GÜVENLİK AÇIKLARI VE ATAK ÇEŞİTLERİ

3.1 GPS Güvenlik Açıkları

ADS-B teknolojisi GPS alıcısı, transponder, barometrik altimetre ve kablolardan oluşur. Bu bileşenlerin her biri potansiyel saldırı riskleri oluşturur. Ancak birçoğu bu araştırmanın kapsamı dışındadır. Üzerinde odaklanılacak saldırılar, bir uçak tarafından iletilen ve alınan ADS-B mesajlarının istismar edilmesini amaçlayan saldırılardır.

2002 yılında Birleşik Devletler Genel Muhasebe Bürosu tarafından yayınlanan bir raporda, GPS'deki mevcut tehditlerin, ticari havacılığa ciddi risk oluşturarak sistemin geçici olarak kesintiye uğramasına neden olduğu vurgulanmaktadır [19]. Yerleşik GPS vericisi ticari bir uçakta yer alan GPS alıcısına müdahale ederek uçağın tüm GPS bilgilerini geçici olarak kaybetmesine neden olabilmektedir. Bir başka çalışmada, GPS mimarisinin aksamalara yatkın olduğunu belirtilmiştir. ADS-B, hava sahasındaki uçakların konumlarını belirlemek için yalnızca GPS'e güvenmektedir. GPS, ADS-B verilerini iletmezse de, GPS teknolojisi içinde, ADS-B gözetim teknolojisinin tümünün işlevselliğini zayıflatabilecek birtakım güvenlik açıkları vardır. GPS sistemi, konum mesajlarının uydulardan uçağa ve yer istasyonuna (örneğin alıcı) gidebilmesi nedeniyle, güvenlik açıklarının farklı seviyelerde oluşabileceği çok karmaşık bir yapıdır [19]. Çizelge 3.1 ve 3.2'de gösterildiği gibi ticari gözetim sisteminin farklı bölümlerinde kasıtsız ve kasıtlı güvenlik açıkları hakkında daha fazla ayrıntı içermektedir.

3.2 ADS-B Güvenlik Açıkları

Herhangi bir ADS-B donanımlı uçak, yerleşik GPS donanımından türetilen konumunu veri iletişim bağlantısıyla yayınlayabilmektedir [20]. Navigasyon sinyalleri için belirlenen frekanslar (örneğin 1090 MHz ve 978 MHz) sinyal engelleme atağına açık haldedir. Bu nedenle, ADS-B, sisteme hayalet uçakların enjekte edilmesine açıktır [21]. Havacılık Kuralı Oluşturma Komitesi (ARC), kötü niyetli bir kullanıcının yayınlanan mesajları kullanabileceği ve küresel havasahasında uçuş rota çatışmaları

Çizelge 3.1 : GPS kasıtsız güvenlik açıkları çizelgesi

	Kasıtsız Tehlikeler	
	Tehdit Türü	**Savunmasız uydu sistemi bileşenleri**
Yeryüzüne dayalı	1- Doğal olaylar (deprem, sel, yüksek sıcaklar) 2- Elektrik kesintileri	Yer istasyonları ve veri bağlantıları
Hava yoluna dayalı	3- Hava ortamı (solar, kozmik radyasyon) 4- Havadaki cisimler (enkaz dahil)	Uydular ve veri bağlantıları
Girişim odaklı	5- Solar aktivite; atmosferik ve solar karışımlar 6- İnsan odaklı kasıtsız girişimler	Uydular ve veri bağlantıları

Çizelge 3.2 : GPS kasıtlı güvenlik açıkları çizelgesi

	Kasıtlı Tehlikeler	
	Tehdit Türü	**Savunmasız uydu sistemi bileşenleri**
Yeryüzüne dayalı	7- Fiziksel zararlar 8- Sabotaj	Yer istasyonları ve haberleşme ağları Tüm sistemler
Hava yoluna dayalı	9- Önleyiciler (uzay madenleri, havadan havaya missillemeler) 10- Yönlendirilmiş enerji silahları (lazer, elektromanyetik darbe)	Uydular ve bağlantıları
Girişim ve içerik odaklı	11-Siber ataklar 12-Sinyal Engelleme	Tüm sistemler ve haberleşme ağları

oluşturabileceği konusunda ciddi endişeler dile getirmiştir [21]. ARC bulgularına yanıt olarak, çeşitli hükümetler, endüstriler ve akademik kurumlar kendi araştırmalarını gerçekleştirmiş ve ADS-B sisteminin minimum güvenlik mekanizmalarından yoksun olduğunu ve Çizelge 3.3'te özetlendiği gibi hem iç hem de dış tehditlere karşı savunmasız olduğunu keşfetmişlerdir.

ADS-B'nin düşük güçte bir sinyalle çalıştığını, bunun GPS ve kablosuz iletişimlere bağımlı olduğunu, dolayısıyla ilkel radardan daha savunmasız olduğunu belirtmek gerekir [22]. Kötü niyetli bir aktör, 24 bit uçak ICAO adresi veya iletişim kuran uçakların seyahat planı gibi gizli bilgilere yönelik bir aramada ADS-B yayını mesajlarını dinleyerek pasif saldırıları gerçekleştirebilir [23]. Aktif saldırılar, iletişim halinde olan tarafları yerleri hakkında kasıtlı olarak karıştırm yaparak sahte verilerden kaynaklanan yanlış yorumlanmasına yol açan hatalı bilgileri bir ADS-B mesajına enjekte etmesine sebep olur [23].

ADS-B teknolojisindeki güvenlik açıkları daha önceki akademik çalışmalarda dile getirilmesine rağmen ADS-B'nin temel mimari ve tasarım sorunları düzeltilmemiştir. Costin, ADS-B sinyallerini taklit etmek için uygun donanım ve yazılım bileşenleri ile ticari olarak uygun maliyetli bir düşman modeli kullanarak hayalet uçakları radar ekranına enjekte etmiş ve bahsedilen kusurları ispatlamıştır. ADS-B donanımlı uçakların mahremiyeti korunamamaktadır çünkü uçak tanımlama, hız ve irtifa gibi bilgiler, www.flightradar.net gibi web sitelerinde kamuya açık yayınlanmaktadır .

3.3 GPS'e karşı bilinen ataklar

GPS'e karşı bilinen ataklar saldırı seviyesi düşük, orta veya yüksek olarak sınıflandırılabilir. Düşük seviyedeki saldırılar, kötü niyetli aktör tarafından sistem mimarisine çok az bilgi vererek ve sisteme çok az zarar vererek oldukça kolay gerçeklenebilir. Orta derecede saldırılar, sistemin çalışabilirliğini bozmak için sistem seviyesinde bilgi gerektiği yerde gerçeklenebilir. Kötü niyetli bir kullanıcı sistem hakkında kapsamlı bilgiye sahipse üst düzey saldırılar yapılabilir.

1090 MHz yayın bağlantısına yapılan saldırıların yanı sıra, yeterli becerilere sahip kötü niyetli kullanıcının uçak ve yer istasyonlarını etkileyen dağıtılmış bilgisayar ağında

Çizelge 3.3 : ADS-B güvenlik açıklıkları

Tehdit Türü	Açıklama	Açıklık
1- 1090 MHz Sinyal Engelleme	- Geçici olarak gönderici ve alıcı arasındaki iletişimi devre dışı bırakır (DoS).	- Ortak bir haberleşme kanalında iletim
2- ADS-B Sinyal Enjeksiyonu	- Hava sahasında gerçek hava taşıtlarını ve hava trafik kontrolörlerini yanıltmak için rastgele hatalı bir sinyal enjeksiyonu gerçeklenir.	- ADS-B yeteneğine sahip herhangi iki cihaz mesaj alışverişi
3- ADS-B Sistem Kapatma	- Uçak izini ve takibini devre dışı bırakır.	- Fiziksel olarak sisteme erişme becerisi
4-Dahili Veri Manipülasyonu ve Bozulması	- Yer istasyonu haberleşme ağını keser.	- Güvenlik duvarları, antivirüs ve saldırı tespit sistemleri eksikliği
5- Sorumluluk Reddi	- Sistem, bozuk bilgi saptadığında, bu tür bilgileri gönderildiğini veya alındığını inkar ederek hava sahası sistemindeki kaza veya arıza sorumluluğunun bozulmasına neden olur.	- Hata kontrol mekanizması eksikliği
6- Mesajı Kötüye Kullanma ve Silme	- Düşman uçakları bulabilir ve takip edebilir. - Yer istasyonları ile hava trafik yönetim sistemi arasındaki iletim sırasında mesaj değişiklikleri - Kontrolör ekranında gerçek zamanlı uçak pozisyonu kaybı - GPS karışıklığı, uçakların GPS kullanma yeteneğini engelleyebilir	- ADS-B özellikli herhangi iki cihaz ileti alışverişinde bulunabilir - Güvenli bir iletişim kanalı eksikliği
7- GPS'de ADS-B Sistem Gereksinimi	- Uçak ve uçak arasında değiş tokuş yapılan hava trafiği ve hava trafik kontrolünün açık verilerini dinleyebilir	- Sinyal engellemesine karşı duyarlılık eksikliği
8- Dinleme	- ADS-B mesajlarını alabilme, değiştirebilme ve yeniden yayınlama olanağı sağlayan üçüncü taraf yetkisi vardır.	-İletişim kanallarındaki güvenlik eksikliği (şifreleme yok)
9- Gecikmeli Sinyal Aktarımı	- Mesaj gizliliği yoktur, uluslararası kullanımı sınırlar.	- Kimlik doğrulama mekanizması eksikliği
10- Güvensiz Veri İletimi	- Uçak pozisyonu ve uçuş numarası halka açıktır.	- Verilerin şifrelenmesi eksikliği
11- Gizlilik, doğruluk ve erişilebilirlik eksikliği	- Eşsiz 24 bit kod uçak tanımlayıcı adresi, halka açıktır. - Uçak kimliği verilerinden ve güncel pozisyon bilgileriyle uçaklara yapılan saldırıyı koordine edilebilir.	- Verilerin şifrelenmesi eksikliği

(ör. NextGen) dahili ve harici saldırıları gerçekleştirebileceğini varsayılmaktadır. Bu bölümde GPS ve ADS-B'nin güvenlik açıklarını ele alınmaktadır.

3.3.1 Yayın Bozma Atağı

Yayın bozma atağı, bir veya birçok ağ düğümünün veya bölgesinin sinyal alışverişini engellemektedir. 1090 MHz frekansında oldukça yüksek güçte sinyal gönderilerek uygulanır. Bu saldırıda kötü niyetli kullanıcı navigasyon sisteminin sinyal iletimine müdahale etmektedir. Böylece alıcı tarafından başarılı bir mesaj alım olasılığı azalır. Sonuç olarak alıcının (örneğin, pilot, kontrolör) uçağın doğru bir konumunu belirlemesi önlenir. SSR ve PSR sistemleri de bu atağın hedefi olabilir ve hizmetin engellenmesine (DoS) sebep olur.

3.3.2 Sinyal Sentezi Atağı

Bu saldırı, alıcıyı (örneğin pilot, kontrolör) yanıltmanın yanısıra, uçağı gerçek konumundan farklı bir konumda göstererek yanlış pozisyon mesajları üretir ve gönderir. Kötü niyetli kişi navigasyon sinyalleri yayınlamak için güç amplifikatörünü ve bir anten kullanır.

Fiziksel ortamda iletim halindeki mesajı deşiştirmek, gölgeleme ve bit değiştirme yöntemleri şeklinde iki farklı yaklaşımla yapılır. Gölgeleme yönteminde kötü niyetli kişi, hedefteki mesajın tamamını ya da bir kısmını değiştirmek amacıyla yüksek güçte sinyal gönderir. Bit değiştirme yöntemi sinyali üst üste bindirerek bit değerlerini değiştirir. Bu iki yöntemde de normal kullanıcıların haberi olmadan, mesaja veri eklenebilir. ADS-B teknolojisinde kimlik doğrulama metodu olmadığı için, uygun bir ADS-B mesajı üretip gerekli modülasyon uygulandıktan sonra atak gerçeklenebilir

3.3.3 Solucan Yuvası (Wormhole) Atağı

Bu saldırı, sinyallerin çeşitli kanallarla kesilmesi ve iletilmesi açısından Sinyal Sentezi Atağı'na benzer. Burada amaç sinyaller toplamak ve sinyalleri gerçek varış noktasına iletmektir. Kablosuz iletimler farklı hızlarda ve rotalarda gerçekleştiği için, alıcılar için sinyal gönderim hızına bağlı olarak tercih edilen seçenek olabilir. Bu durumda, pilot,

hatalı sinyalleri kabul edecek ve ilgili uçağın gerçek pozisyonuyla ilgili yanlış karar verecektir.

3.3.4 Seçici Gecikme Atağı

Radyo frekansına dayalı konumlandırma sistemleri, konumlarını yayınlanan sinyallerin varış zamanı (TOA) cinsinden hesapladığından, kötü niyetli bir kullanıcı seçici gecikmeli bir saldırı gerçekleştirebilir. Bu kişi, her navigasyon sinyalini alıcı tarafından yanlış bir pozisyon hesaplayacak şekilde düşürebilir. Böylece tüm kapsama alanına atak yapan kullanıcının kendi oluşturduğu trafiğin atak yaptığı sisteminin parçası bir trafikmiş gibi göstermesine izin verilmiş olur.

3.3.5 Sahte Düzeltme Atağı

Sahte Düzeltme Atağı, düzeltme mesajlarını yakalayan ve doğrudan değiştiren bir saldırı tarzıdır. Kötü niyetli kullanıcı, referans istasyonlarına yönelik yaptığı saldırı sonucunda yanlış düzeltme mesajları üretmesine neden olur. Sahte düzeltme mesajlarını elde eden bir pilot yanlış bir konum hesaplar.

3.3.6 İzleme Noktası Kaydırma Atağı

Sinyalin zamanında gelmesi, global konumlandırma sistemleri literatüründe izleme noktası olarak bilinir. Bir düşman, orijinal darbenin üzerine bir değiştirme sinyali ekleyerek izleme noktasını manipüle edebilir, böylece alıcı yanlış bir izleme noktasını tanımlar.

3.3.7 Alıcıya Yapılan Sabotaj Atağı

Bir düşman, hava tradiği altyapısına fiziksel erişim kazandığı takdirde, yazılım ve donanım güncellemeleri alıcı üzerinde yürütülebilir. Bu müdahale, alıcının yanlış hesaplanmış konumlar görüntülemesine neden olabilir.

3.3.8 Gizli Anlaşma Atağı

Bir grup kötü niyeli kullanıcılar, değiştirilmiş mesajları sisteme enjekte etmek ve meşru iletişimi güçlendirmek için birlikte çalışırlar. Amaç, hedeflenen alıcının mesaj

gönderip cevap alamamasını sağlamaktır. Buna ek olarak, hedeflenen alıcı kötü niyetli olarak raporlandırılabilir.

3.4 ADS-B'ye Yönelik Ataklar

Otomatik Bağımlı Gözetim-Yayıncılığı sayısal mesajları iki farklı frekans, 1090-MHz ve 978-MHz'de göndermektedir. Bu bölümde yapılan çalışma doğrultusunda yalnızca 112 bit uzunluğunda ve 56 bitlik ADS-B bilgileri içeren 1090-MHz yayın bağlantısına yapılan saldırılara odaklanılmıştır.

3.4.1 ADS-B Mesajı Bozma Atağı

GPS okumalarının uzaktan manipüle edilmesinin, uçakların ekranında yanlış konum verisine yol açabileceği bir saldırı tipidir. Bozuk bilgilerle, kötü niyetli kullanıcı uçuşları ertelebilir ve yanlış trafik bilgileri türetebilir.

3.4.2 ADS-B Mesajı Kötüye Kullanımı Atağı

Pasif dinleme yapan kötü niyetli kullanıcı, uçakları çok yüksek doğrulukla tespit edebilir ve takip edebilir. Bu tür saldırı tipleri yan kanal saldırısı olarak adlandırılır ve uçaklar ile yer istasyonları arasındaki haberleşme verilerini yakalayarak bir uçağın yakıt düzeyini kötü niyetli kişilerin kullanımına maruz bırakabilir. Dahası, uçağın gerçek zamanlı hareketi, kamuya açık veritabanına erişime açık halde olmasından ötürü etkilenebilmektedir.

3.4.3 ADS-B Mesajı Geciktirme Atağı

ADS-B hizmetlerini aksatmak için uçak kablosuz iletişimlerinde kasıtlı bir şekilde mesaj iletimini yavaşlatarak yapıldığı bir saldırı tipidir. Dolayısıyla uçakları hava trafik ekranında görselleştirme kaybına yol açar.

3.4.4 Yanlış Alarm Atağı

Kötü niyetli kullanıcı, sistemin düzgün çalışmasını engellemek, yanlış alarmlar oluşturmak ve uçuş gecikmelerine yol açarak sistemde geç tespit yapılmasına neden olmak için hava trafiği iletişimine müdahale etme girişiminde bulunabilir. Kötü niyetli kullanıcı uçakların ayarlama sistem yazılımına kasıtlı olarak hatalı alarmlar

enjekte eder ve uçağın yapılandırmasının hatalı olmasına, dolayısıyla yetkisiz uçuş gecikmelerine neden olabilir.

3.4.5 Uçak Keşif Atağı

Bu saldırıda bir düşman ADS-B mesajlarını yakalar, tanır ve yorumlar. Böylece, bir kötü niyetli kullanıcı, hedefleri küresel havasahasında tanımlayabilir.

3.4.6 Yer İstasyonunda Bilgi Akışının Reddi Atağı

Yer istasyonuna odaklanıldığında, bir düşman ucuz bir karıştırma aygıtı kullanarak ADS-B veri bağlantısını (örneğin 1090 MHz) karıştırabilir. Bu şekilde bir düşman sadece yer istasyonu için tasarlanmış olan ADS-B sinyallerinin iletimini kesebilir, ancak tüm yayın sinyallerini kesememektedir.

3.4.7 Hava Aracında Bilgi Akışının Reddi Atağı

Bu saldırı türü, kötü niyetli kullanıcının gerçek zamanlı olarak uçakların konumuna yakın hedefler üretmesini sağlar. Böyle bir durumda, kötü niyetli bir kullanıcı uçakların iniş, kalkış ve vergilendirme operasyonlarını bozmak için sinyal engelleme cihazını kullanacaktır.

3.4.8 Yer İstasyonu Hayalet Hedef Enjeksiyonu Atağı

Kötü niyetli bir kullanıcı, ADS-B sinyalinin orijinal parametrelerini değiştirebilir ve yer istasyonuna saldırmak üzere tasarlanan kötü niyetli dizeleri takabilir ve bu nedenle, hava trafik denetimi için denetleyicinin kullandığı ekranda hayali uçaklar enjekte ederek karışıklığa neden olabilir.

3.4.9 Hava Aracında Ağ Hedefli Kötü Amaçlı Yazılım Atağı

Bu saldırı türü, yolcuların taşıdıkları kablosuz elektronik cihazları hedef almaktadır. Kötü niyetli bir kullanıcı uçak sistem arabirimlerine potansiyel olarak erişebilen, dolayısıyla arabirimlerin çalışabilirliğini kötüye kullanan yolcu cihazlarına erişmek için uçak ağını kullanabilir. Veri bilgisini çalabilen, antivirüs ve izleme araçlarından gizleyebilen bir solucan türü kullanılmaktadır. Kötü niyetli kullanıcı bu solucanı,

ağ mimarisi hakkında bilgi toplamak ve hassas aviyonik verileri elde etmek için kullanabilir.

3.4.10 Yazılım Uyumsuzluğu Atağı

Bu saldırı, kötü niyetli bir kullanıcının yazılım dağıtımını durdurmasını sağlar. Uçak sistemlerinin çalışması için tasarlanmış yazılım güncellemelerini manipüle etme şansını elde etmektedir. Bu sebeple yazılım güncellemelerini başarıyla gerçekleştiremeyen uçaklar uyumsuzluk sebebiyle doğru verileri alıcıya aktaramamaktadır.

3.5 Atak Analizi

Çizelge 3.4'te gösterilen bulgulara göre, GPS gelecekte birincil hava seyrüsefer hizmeti olarak kullanılacaksa güvenlikle ilgili daha fazla teknolojik gelişmelere ihtiyaç olduğu açıktır. Güvenlik açıklarının kombinasyonu, her GPS ölçümüne ciddi belirsizlik verebilir ve ADS-B sisteminin uçakların doğru konumunu belirleme yeteneğini zayıflatabilir. Bu nedenle küresel hava sahasında birtakım hasarlara neden olur. Uçuş rotası çatışmaları gibi istenmeyen sonuçlardan kaçınmak için uçuş verisinin gizliliğini, bütünlüğünü ve kullanılabilirliğini koruyan ADS-B savunma teknikleri gereklidir. Bu savunma teknikleri (örneğin, saldırı tespit sistemi, vb.), ADS-B'ye istenmeyen değişiklikler uygulandığında oluşabilecek riskleri proaktif olarak belirleyecektir. Aksi takdirde, ADS-B ve NextGen'in yetenekleri tehlikeye atılabilir ve Hava Trafik Yönetimi amaçlanan şekilde çalışmayabilir.

Çizelge 3.4 : Atak karşılaştırma

Atak Tipi	Açıklama	Etkisi	Gizlilik	Bütünlük	Gerçeklenebilirlik
GPS'e yönelik ataklar	Yayın Bozma	Düşük			X
	Sinyal Sentezi	Düşük		X	
	Wormhole	Orta		X	
	Seçici Gecikme	Orta		X	
	Sahte Mesaj Düzeltme	Yüksek	X	X	
	İzleme Noktası Kaydırma	Yüksek		X	
	Alıcı Sabotajı	Orta		X	
	Gizli Anlaşma	Yüksek		X	X
ADS-B'ye yönelik ataklar	Mesaj Bozma	Orta	X	X	X
	Mesajı Kötüye Kullanma	Düşük	X	X	
	Mesaj Geciktirme	Düşük			X
	Yanlış Alarm	Orta		X	X
	Uçak Keşif	Düşük	X		
	Yer İstasyonu Bilgi Akışının Reddi	Düşük			X
	Hava Aracı Bilgi Akışının Reddi	Orta		X	
	Yer İstasyonu Hayalet Hedef Enjeksiyonu	Orta Yüksek	X	X	
	Kötü Amaçlı Yazılım	Orta	X	X	
	Yazılım Uyumsuzluğu	Orta	X	X	

4. ÖNERİLEN GÜVENLİK YÖNTEMLERİ ve ANALİZİ

4.1 Sistem Gereksinimlerinin Belirlenmesi

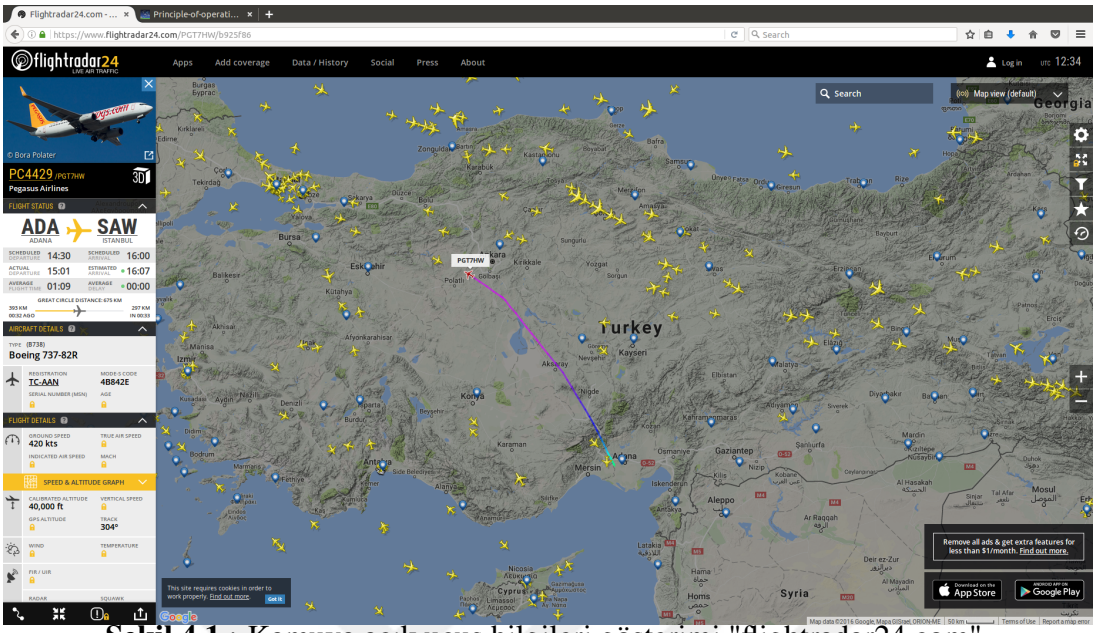
Hava aracı, konumunu, hızını ve yönünü yüzlerce milisaniyede bir periyodik olarak açık metin halinde yayınlamaktadır. Kaybedilen paketlerin normalde bir soruna neden olmamasından dolayı, güvenilirlik önemli bir husustur. Sinyali gönderen herhangi bir paketi tekrar gönderemez ve doğruluğunun garantisi verilememektedir. Protokol üzerinden yapılan ataklar yüksek katmanlarda ele alınır. Paket hatası oranının yan kanaldan bağımsız olarak ortalama %33 civarında seyretme eğiliminde olduğu yansıtılmıştır. Fiziksel katmanda zorunlu ADS-B yayını nedeniyle önümüzdeki dönemde kanal kullanımının artması muhtemel bazı paket kaybı oranının artacağı anlamına gelir. Özellikle yüksek yoğunluklu hava sahalarında giderek artan uçuş trafiği ile bu oran daha da artacaktır [21].

Bağımsız olarak konuşlandırılmış kablosuz (sensör) ağların aksine, keşfedilmemiş sahte ağ birimlerinin fiziksel olarak yakalanması önemli bir konudur. Yasal olarak meşru bir ADS-B birimine erişim olanağı, genel havacılık yöntemleri hesaba katıldığında çok zor görülmemektedir. ADS-B sisteminin kötüye kullanıma hazır haldeki ucuz donanımlar ile yakın zamanda literatürde ADS-B'nin zayıf noktaları keşfedilmiştir. ADS-B için gizlilik ve bütünlüğü sağlayan bir güvenlik planı oluşturmak gerekir.

4.1.1 Gizlilik

Gönderici ile alıcı arasında veri alışverişini yetkisiz bir alıcı engellediğinde, haberleşmenin gizliliği kaybolmaktadır. Havacılıkta, verilerin güvensiz bir şebekede iletilmesi durumunda hassas bilgilerin yetkisiz erişime karşı korunması, olası yolsuzluk ve gizlilik maruziyeti nedeniyle önemlidir. ADS-B verileri bir ağda şifrelenmeden 1090 MHz'de güçlü antenler ile iletilebilmektedir. Böyle bir ağ yapılandırmasıyla, ADS-B özellikli herkes bu verilere erişebilir (örneğin, uçuş

numarası, uçak konumu, 24 bit uçak adresi vb.) ve Şekil 4.1'deki gibi web sitelerinde kötü amaçla kamuoyuna açık hale getirebilir.



Şekil 4.1 : Kamuya açık uçuş bilgileri gösterimi "flightradar24.com".

Güvenlik protokolleri, veri ve kaynak bütünlüğü ve dogruluğu, standartlara uygunluğu, hata düzeltimi, DoS ataklarına karşı güvenliği, uçuş trafik yogunluğu ve hava aracı artışına karşı kolay ölçeklenebilirliği sağlamalıdır [24]. ADS-B güvenliğinin geliştirilmesi ve kablosuz sensör ağı güvenliğinde kullanılan yayın kimliklendirme üzerine de birçok çalışmalar yapılmıştır. Bazı fikirlerin doğrudan ADS-B'ye uygulamak mümkün değildir. Bu bölümde güvenlik yöntemlerinden ve ADS-B'ye uygulanabilirlerinden, avantajlarından ve dezavantajlarından bahsedilmektedir.

4.1.2 Bütünlük

Yetkisiz bir kişi iletim sırasında kullanıcıların gönderdiği verileri değiştirdiğinde sonuç bütünlük kaybı olarak tanımlanır. Bütünlük ve doğruluk hava trafiği kontrolü için özel bir önem taşır. Çünkü yer istasyonu ile uçak arasındaki mesajlar değiştirilebilir veya silinebilir ve uçakların ekrandan kaybolmasına ve sahte mesajların iletilmesine neden olabilir. Başka bir deyişle, pilot ve kontrolör, yanlış kararlar vermelerine yol açan değiştirilmiş verileri alır ya da hiç bilgi almazlar. ADS-B'de yayınlar hedeflerine ulaştığında hiçbir onay alınmamaktadır. Böyle bir ortamda, kötü niyetli bir kullanıcı, mesaj trafiğini taklit edebilir ve değiştirebilir ve böylece ağ güvenliğinin temel özelliklerinden birini ihlal edebilir. Kablosuz iletişimde bir

mesajın bütünlüğünü sağlamak ve hasarlı mesajları tespit etmek için CRC32 bütünlük sağlama mekanizması kullanılabilir [8]. Ek olarak, iki istasyon arasında iletişim gerçekleşmeden önce senkronizasyon (SYN), senkronizasyon-onay (SYN-ACK) ve onaylama (ACK) mesajları değiş tokuş edilir. Bu yöntem, alıcının doğru sırayla yeniden birleştirerek değiştirilmemiş verileri aldığını garanti eder.

- *Veri bütünlüğü:* Verinin, gönderen tarafından sağlananla aynı olmasını sağlar ve herhangi bir üçüncü taraf tarafından değiştirilmemiştir.
- *Kaynak bütünlüğü:* Bir mesajın, gönderildiğini iddia eden katılımcının kaynaklandığından emin olun.
- *Veri kaynaklı kimlik doğrulaması:* Bir iletinin, bir iletide talep edilen konumdan kaynaklandığından emin olun.
- *Mevcut işlemler üzerinde düşük etki:* Bir şema, mevcut ADS-B kurulumlarıyla uyumlu olmalı ve hem sabit hem de yazılım standartlarını aşırı derecede etkilememelidir.
- *Ölçeklenebilirlik:* Herhangi bir yaklaşımın kolayca ölçeklenebilir olması gerekir. Bu, yerel olarak yükselen bir uçak yoğunluğu ve küresel olarak artan uçak trafiği açısından geçerlidir. Ağır şekilde kullanılan 1030 MHz kanalındaki yük artmamalıdır.

4.2 Güvenlik Yöntemleri

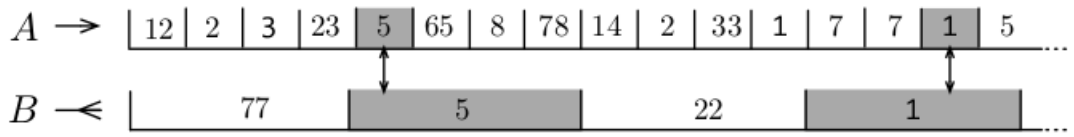
ADS-B'ye yönelik muhtemel saldırıları mühendisler ve akademisyenler tarafından önerilen güvenlik yöntemlerini vurgulamak gerekmektedir. Bu bölümde, bir önceki bölümde analiz edilen atak çeşitlerinin birlikte gruplandığı ve saldırı zayıflatma tekniği kullanıldığı genel yaklaşımlar incelenecektir.

4.2.1 Makine Öğrenmesi

Şimdilik¸ ADS-B güvenliğini gelştirmek amacıyla kriptografik olmayan metotlar üzerine uygulamalar gerçeklenmemiştir. Ancak şüpheli durumları algılamak amacıyla örüntü tanıma metodları uygulanabilir. Normal kullanıcı ve kötü niyetli kullanıcının fiziksel katmandaki paketlerde belirgin farklılıkları varsa, normal davranışları tahmin

edebilecek bir makine öğrenmesi yöntemi geliştirilebilir. Belirli bir eşik değeri üstündeki veya altındaki aktiviteler şüpheli olarak algılanabilir [25].

4.2.2 Eşgüdümsüz Frekans Atlamalı Yöntemi



Şekil 4.2 : Frekans atlamalı yöntem veri şeması.

Eşgüdümsüz frekans atlamalı yöntemde, kablosuz ağların dar bant sinyal engelleme ataklarına karşı güvenlik sağlayabilmesi amaçlanmıştır. Normalde daha önceden paylaşılmış frekanslarda anlaşma sonucu sinyal frekansı atlamalı olarak gerçeklenir. Askeri yöntemlerde (TACAN ve TDL sinyallerinde) sıklıkla kullanılır. Koordine olmamış rastgele frekans atlamalarındaki önemli nokta, gönderici ve alıcının aynı anda aynı kanalda olma olasılığıdır [26]. Ancak ADS-B gibi büyük ölçekli sistemlerde rastgele frekans atlamalı yöntem düşük performans sergileyecektir. Eşgüdümsüz frekans atlamalı yöntemde bir saldırganın ilgili frekansı dinlemeden paketi elde etme olasılığı formülü aşağıdaki gibidir.

$$p_m \geq 1 - (1 - \frac{c_s}{c})^{c_r} \tag{4.1}$$

c olası kanalların sayısı,

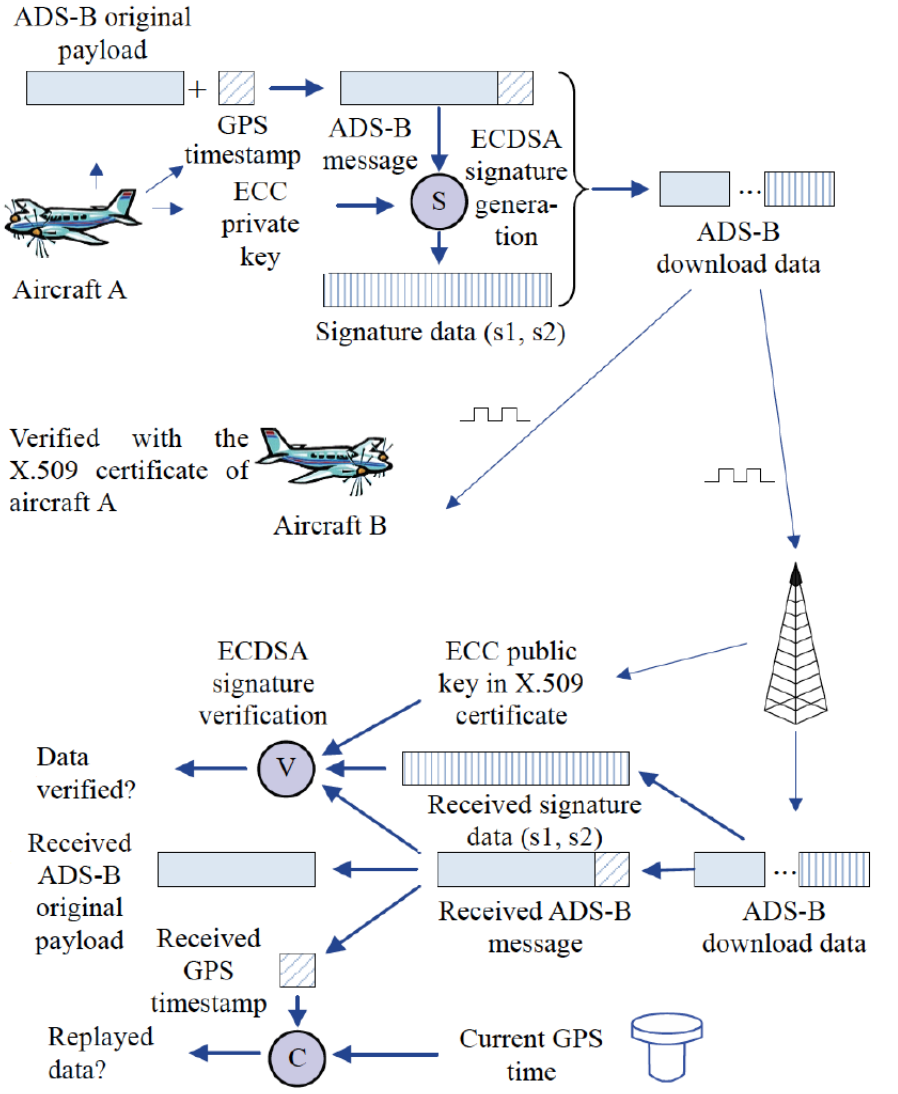
c_s gönderenin aynı anda kullandığı kanalların sayısı,

c_r alıcının aynı anda kullandığı kanalların sayısı

4.2.3 Kriptografik Yöntemler

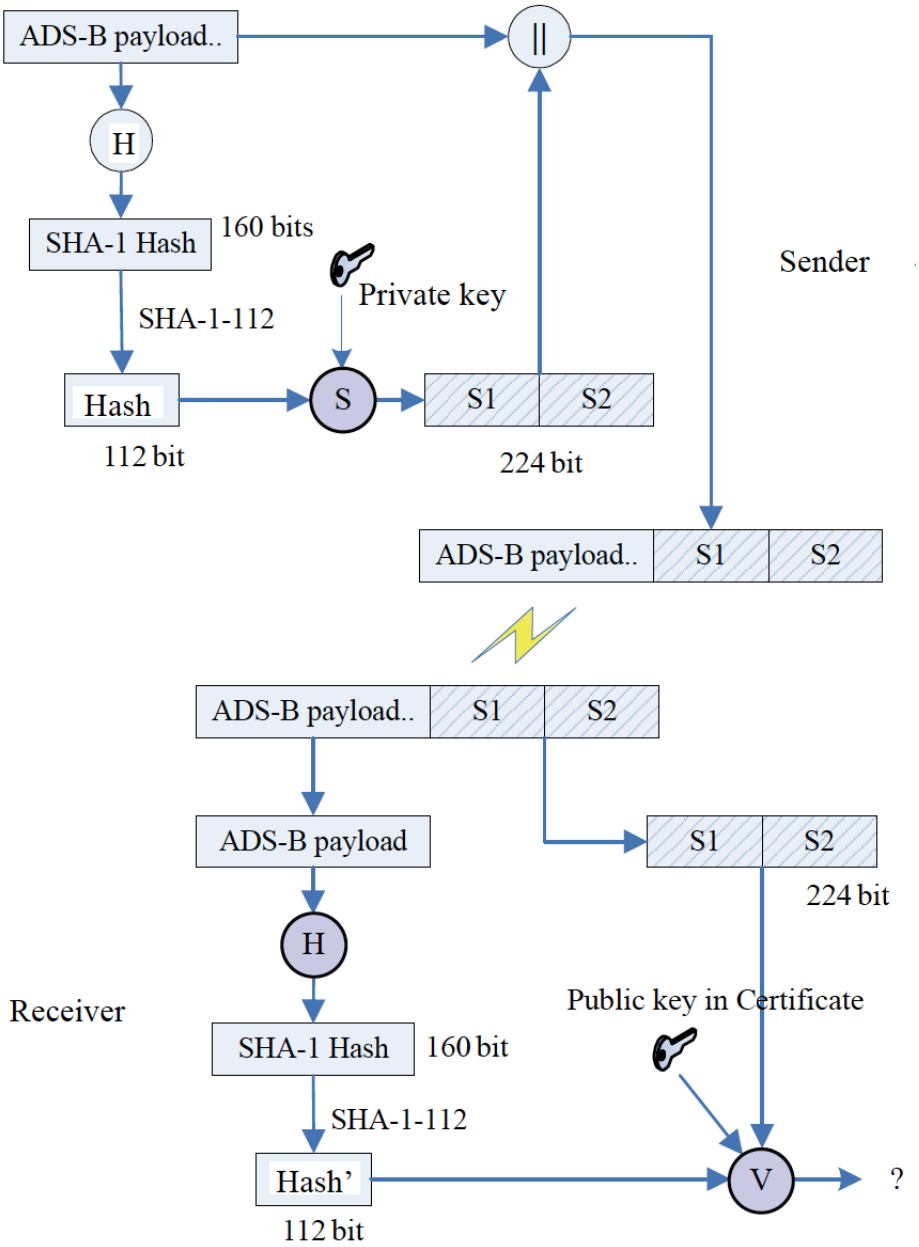
Yayın ortamında mesajların kimlik doğrulaması zordur. Alıcının, mesaj sahibinin kimliğini doğrulaması için asimetrik şifreleme mekanizması gerekir. Hava araçlarındaki alıcılar ve yeryüzündeki istasyonlar için basit açık anahtarlı kriptografik (PKI) yöntemlerin gerçeklenmesi kısa ve uzun vadeli güvenlik çözümüdür. Yerine geçme ataklarına karşı kimlik doğrulamalı güvenlik ancak PKI tarafından sağlanabilir [21]. Basit PKI uygulamalarını gerçeklemek için daha kısa anahtar uzunlukları,

yayın ortamının band genişliğine uyumlu ve hesaplama karmaşıklığı basit olması gerekmektedir. İlk olarak ADS-B güvenliğini artıracak en basit geliştirme, ADS-B mesajlarına bütünlük doğrulaması eklemektir. Sertifikalı bir ADS-B cihazı, imza anahtarlarındaki Sertifika Otoritesi(CA) dizilerini kullanarak diğer hava araçları yayınlarının geçerliliğini güvenli bir şekilde doğrulayabilirse mesaj injeksiyonu metoduna karşı güvenlik sağlanır [27].



Şekil 4.3 : ADS-B için Eliptik Eğri Kriptografisi Şeması.

X.509 sertifikasına dayalı bir ADS-B sistemi için veri doğrulama çözümü önerilmiştir [28]. Veri tekrarlama saldırılarına karşı koruma sağlamak için GPS bilgisinde zaman damgası verilerini kullanan veri doğrulama için bir çözüm önerilmiştir. Orijinal ADS-B sinyaline ek olarak zaman damgası verisinin eliptik eğri şifreleme (ECC) özel anahtarı ile Elliptik Eğri Veri İmzası Algoritması (ECDSA) olarak adlandırılan bir algoritma tarafından imzalanması gerekmektedir. İmza verileri, yeni imza verilerine



Şekil 4.4 : ADS-B için Eliptik Eğri Kriptografisi Şeması.

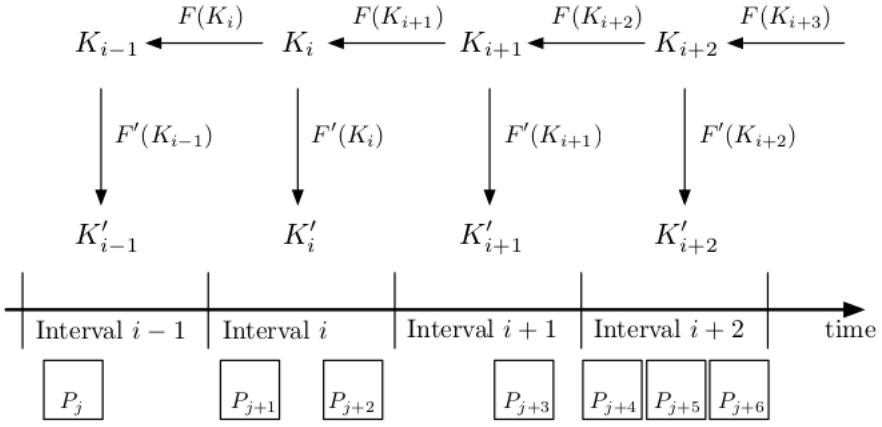
uyacak şekilde tanımlanacak olan ADS-B çıkışı adı verilen yeni bir veri türüne kapsüllenir. Yeni veriler, ADS-B iletişim kanalı vasıtasıyla orijinal veriler ile birlikte gönderilecektir. İmza esaslı alınan mesajın kaynaktan gönderilen orijinal mesaj olduğundan emin olunması sağlanmaştır. Bu çözümün fizibilitesi, henüz gerçek bir uçak üzerinde test edilmediğinden ispat edilememiştir. Yapılan laboratuvar testleri, çözümün ADS-B verilerinin doğrulanması için geçerli olduğunu kanıtlamıştır [28].

ADS-B güvenliğini arttırmak üzere asimetrik şifrelemede eliptik eğrinin kullanıldığı sistem önerisi Şekil 4.4'deki gibidir . Ancak burada zaman damgası ADS-B mesajına eklendiği için mesaj formatı değişmektedir, dolayısıyla uygulanabilirliği zayıftır.

4.2.4 Geriye Dönük Anahtar Yayınlama Yöntemi

Geleneksel asimetrik şifrelemenin bir varyasyonu olarak, göndericilere anahtarlarını geçmişe dönük olarak yayınlama tekniğidir ve daha sonra yayın iletilerinin kimliğini doğrulamak için alıcılar tarafından kullanılır. Herhangi bir yayın organı, daha sonra her mesajla birlikte gönderilen şifrelenmiş bir mesaj kimlik doğrulama kodu (MAC) üretir. Belirlenen miktarda zaman veya mesajdan sonra, bu MAC'in şifresini çözmek için anahtar basılır. Önceki mesajları arabelleğe koyan tüm dinleyen alıcılar, şimdi iletilerin şifresini çözebilir ve gönderenin zamanla devamlılığını sağlayabilir.

Standartlaştırılan TESLA (Zamana Uygun Verimli Akış Kaybı Toleranslı Kimlik Doğrulama) protokolü, paket kayıp sorunları baş edebilmekle birlikte, büyük ölçekte verimli yayın kimlik doğrulaması ve gerçek zamanlı sistemlere uygulunabilirliği sağlamaktadır. Şekil 4.5'de görüldüğü gibi μTESLA yayın kimlik doğrulama protokolü, kablosuz sensör ağları için TESLA protokolünün uyarlamasıdır.



Şekil 4.5 : μTesla protokolü şeması.

μTESLA protokolü Şekil 4.5'de gösterildiği gibi tek yönlü anahtar zincirleri kullanmaktadır. Gönderici, rasgele bir anahtar K_n seçer ve anahtarları elde etmek için gereken rasgele fonksiyon F'i uygular: $K_i = F(K_{i+1})$, $0 \leq i \leq n-1$ Daha sonra gizli anahtarları $K_i, i > 0$, i. inci aralıkta göndermektedir. $i < j$ olan her K_i, alıcı tarafından

tek yönlü bir F fonksiyonu kullanılarak kurtarılabilir [29]. Alıcının mesaj kimliğini doğrulamak için iki şey yapması gerekir:

1 Aynı anahtar zincirinden olduklarından emin olmak için daha önce alınan anahtarlara karşı K_i anahtarını onaylamalıdır,

2 Anahtar K_i'ye sahip mesajın, anahtar yayınlanmadan $i+d$ aralığından önce gönderildiğinden emin olunmalıdır.

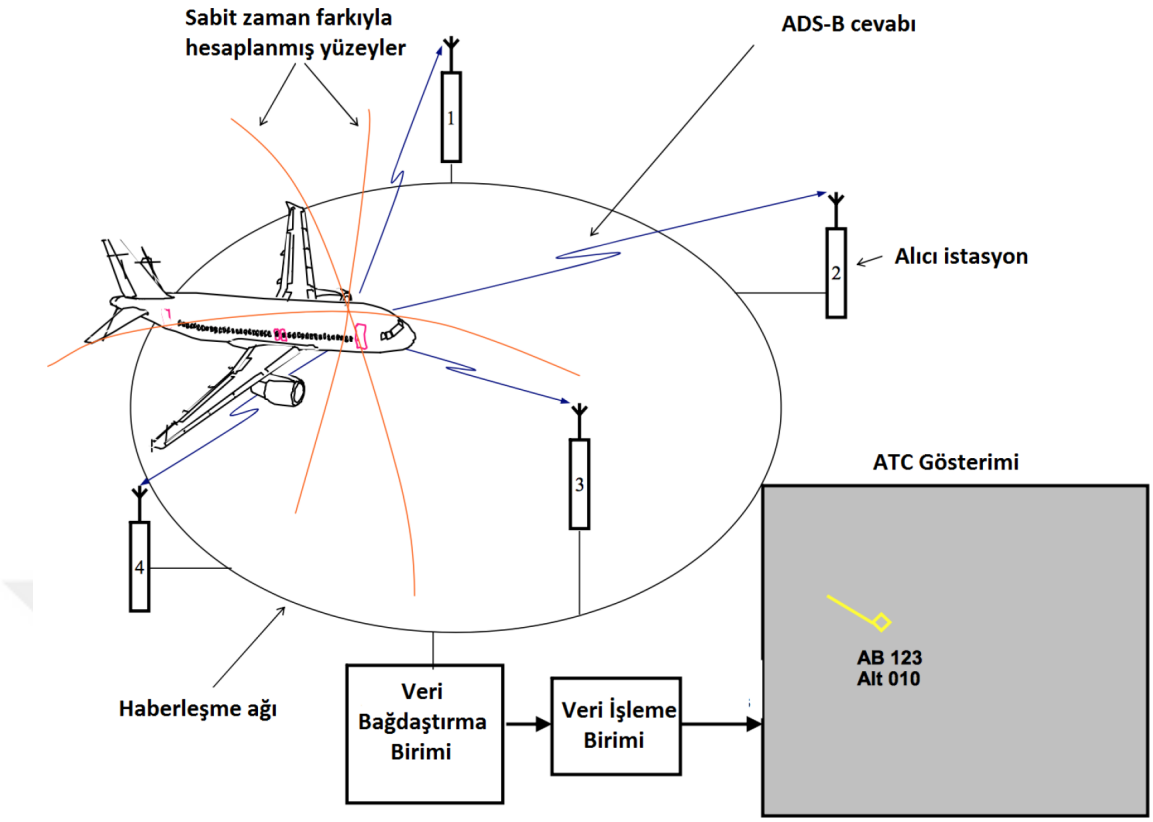
μTESLA'nın zamanla bağlantılı olarak simetrik şifreleme kullanması, ADS-B'ye adaptasyonunu kolaylaştırmaktadır çünkü GPS vasıtasıyla yeterli zaman senkronizasyonu sağlanabilir [29]. ADS-B yayın niteliğini korur. μTESLA protokolü gerçeklendiğinde, uygulama aşamasında kimlik doğrulama sonucu ve kaynak bütünlüğü uygunsa, göndericinin sürekliliğini sağlamak için karmaşık bir PKI altyapısına ihtiyaç duyulmamaktadır. Ayrıca yerine geçme saldırılarına karşı kullanıcıların bilgilerini koruyabilmesini sağlar.

μTESLA'nın diğer bir avantajlarından biri de 1090 MHz frekans bandındaki kayıp paketlerin kimlik doğrulama için vazgeçilmez olmayışıdır. Yani kayıp paketler sonradan elde edilebilir. Dolayısıyla iletişim masrafları ve ADS-B protokolünde gerekli minimum değişiklikler, geleneksel asimetrik şifreleme yöntemlerinden çok daha azdır [29].

4.2.5 Çoklu Algılama ve Konumlama Yöntemi

ADS-B'de haberleşme güvenliği dışında, hava trafik yönetiminde bütünlük, doğruluk sağlayabilmek amacıyla güvenli lokasyon doğrulama yaklaşımları da vardır. Yani hava aracından gelen irtifa bilgilerini de farklı ADS-B kaynaklardan doğrulamak gerekir.

Birden çok kaynaktan irtifa bilgilerini almak, hava aracının konumunu belirlerken avantaj sağlar. Şekil 4.6'te hedefin 3 boyutlu konumladırmasını yapabilen 4 alıcılı çoklu algılama ve konumlama yöntemi gösterilmiştir. Çoklu algılama ve konumlama yönteminde SSR ve ADS-B sinyallerini kullanarak hava aracının iki veya üç boyutlu konumlandırılmasını sağlar. Dolayısıyla ADS-B mesaj içeriğinde bulunan GPS konum verisine ihtiyaç duyulmaz.

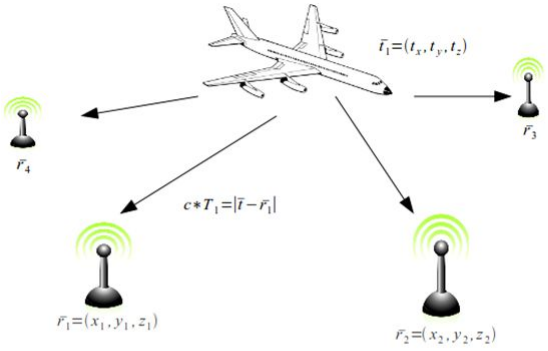


Şekil 4.6 : TDOA - 4 alıcılı senaryo.

4 farklı sensörün farklı pozisyonlara konumlandırılmasıyla göndericiden gelen sinyal alıcılara farklı zamanlarda ulaşır. Zaman farklarının kullanılarak gönderenin 3 boyutlu pozisyonunu veren denklem Şekil 4.7'teki gibi oluşturulur. Farklı iki alıcının zaman farkını kullanarak üç boyutlu uzayda hedefin konumu için hiperbol kestirimi yapılır. Kalan alıcıların zaman farkından oluşturulan hiperbollerin kesişimlerini kullanarak hedefin konumu Şekil 4.8'teki gibi belirlenebilir

Çoklu algılama ve konumlama yöntemi, temelde uçakların takibinde doğruluğu artırmak için ordu ihtiyaçlarını gidermek için geliştirilen bir teknolojidir. Stratejik bölgede bulunan birçok yer istasyonu tarafından uçaklar için Varış Zaman Farkı'nı (TDOA) ölçmeyi içerir. Bu istasyonlar sorgu sinyalleri gönderir ve cevapları dinler. Yanıtlar, uçak ve yer istasyonları arasındaki mesafe farkı nedeniyle birçok farklı istasyona farklı zamanlarda ulaşmaktadır. Zamanlama bilgilerinden uçağın pozisyonu hassas bir şekilde belirlenebilir ve diğer uçaklara iletilebilir.

Yer istasyonu ve hava aracı, herhangi bir uçağın konumunu başarılı bir şekilde doğrulayabilir. Dolayısıyla kötü niyetli bir kullanıcının herhangi bir uçağın konumunu diğer uçaklara veya kontrol kulesine iletmesini önler. Sistemin doğruluğu hedefin alıcı

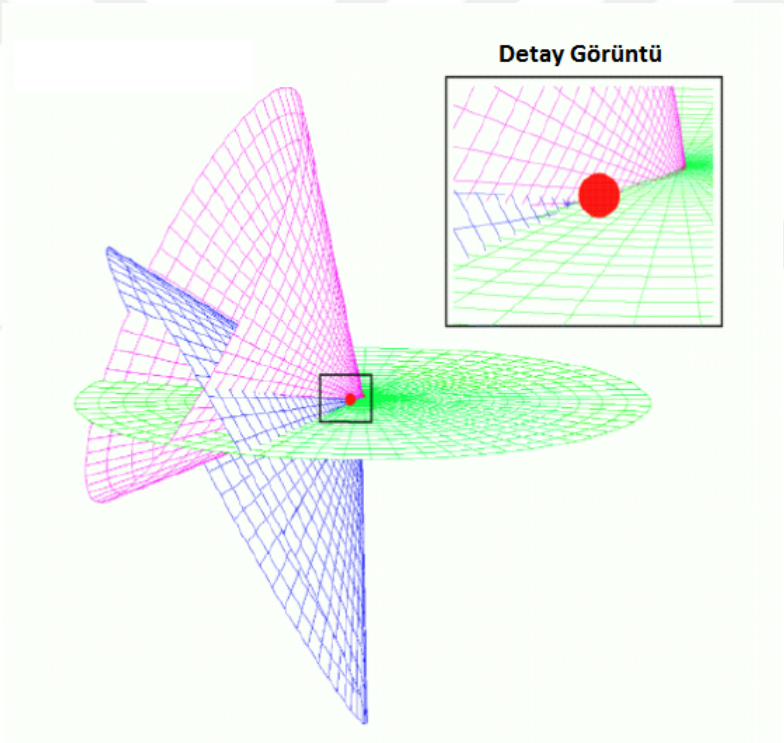


TDOA – Time Difference of Arrival

$$\begin{bmatrix} 0 \\ T_{diff,1} \\ T_{diff,2} \\ \cdots \\ T_{diff,N} \end{bmatrix} = \begin{bmatrix} T_{abs,0} \\ T_{abs,1} \\ T_{abs,2} \\ \cdots \\ T_{abs,N} \end{bmatrix} - \begin{bmatrix} T_{abs,0} \\ T_{abs,0} \\ T_{abs,0} \\ \cdots \\ T_{abs,0} \end{bmatrix}$$

$$c \cdot \begin{bmatrix} 0 \\ T_{diff,1} \\ T_{diff,2} \\ \cdots \\ T_{diff,N} \end{bmatrix} = \begin{bmatrix} |\bar{t}-\bar{r}_0| - |\bar{t}-\bar{r}_0| \\ |\bar{t}-\bar{r}_1| - |\bar{t}-\bar{r}_0| \\ |\bar{t}-\bar{r}_2| - |\bar{t}-\bar{r}_0| \\ \cdots \\ |\bar{t}-\bar{r}_N| - |\bar{t}-\bar{r}_0| \end{bmatrix}$$

Şekil 4.7 : TDOA - 4 alıcılı denklem.



Şekil 4.8 : TDOA - 4 alıcıyla oluşan 3 hiperboloidin kesişimi.

istasyonlarla birlikte oluşturduğu geometriye ve alıcılar arası zaman senkronizasyon hatasına bağlıdır. Bu sebeple istasyonlar arasında nanosaniyeler mertebesinde zaman senkronizasyonu sağlanması gerekir.

Çoklu algılama ve konumlama yöntemi, birçok yer istasyonu içerdiği için pahalıdır ve genelde ordu tarafından uygulanabilmektedir. Çoklu algılama ve konumlama yönteminin başarılı örneklerinden biri de Japonya'daki Narita Uluslararası

havaalanıdır. Burada, havaaracı kontrolörlerine doğru ve son derece güvenilir gözetim bilgileri sağlayarak, havaalanında güvenli ve sorunsuz operasyonlar sürdürülmektedir [30].

4.2.6 Mesafe Bazlı Protokoller

Masefe bazlı haberleşme protokolleri, kablosuz ağlarında güvenli konumlandırma ve erişim izni için kullanılmaktadır. Amaç alıcının, erişim izni isteyen kullanıcıya uygun mesafede olup olmadığını kriptografik biçimde kanıtlamasıdır.

Mesafe bazlı protokollerin güvenliği elektromanyetik dalgaların ışık hızında ilerlediği gerçeğine dayanır. Göndericinin yakınlığını test etmek amacıyla seri sorgu-cevap haberleşmesi esnasındaki geçen zaman kısıtlanmaktadır. Sistemi yanıltmak isteyen bir kullanıcı, bulunduğu mesafeden daha yakında olduğunu belirterek sistemi yanıltamamaktadır. Çünkü uygun zaman koşulunu sağlayabilmek için sorguları bilmeden cevapları göndermesi gerekir [31]. Ancak kötü niyetli bir kullanıcı, bit sorgularına karşılık gelen uygun cevapları uygun gecikmelerle gönderdiğinde, bulunduğu mesafeden daha uzakta olduğunu belirterek sistemi yanıltabilir. Mesafe bazlı protokollerinin yakınlığı ispatladığı temel fonksiyonları incelemek üzere Hancke Kuhn protokolüne değinmek gerekir.

4.2.6.1 Hacke Kuhn Protokolü

Hancke-Kuhn protokolü yavaş ve hızlı faz olmak üzere iki bölümden oluşmaktadır. Protokol kimlik doğrulama yanında gönderilen bir bitin gidip gelme süresinden faydalanarak etiket ile okuyucu arası mesafeyi belirler. Okuyucunun gönderdiği bir bitin sonucunda etiketin bu biti kullanıp tekrar okuyucuya ulaşma süresi aşağıdaki denklem ile hesaplanır.

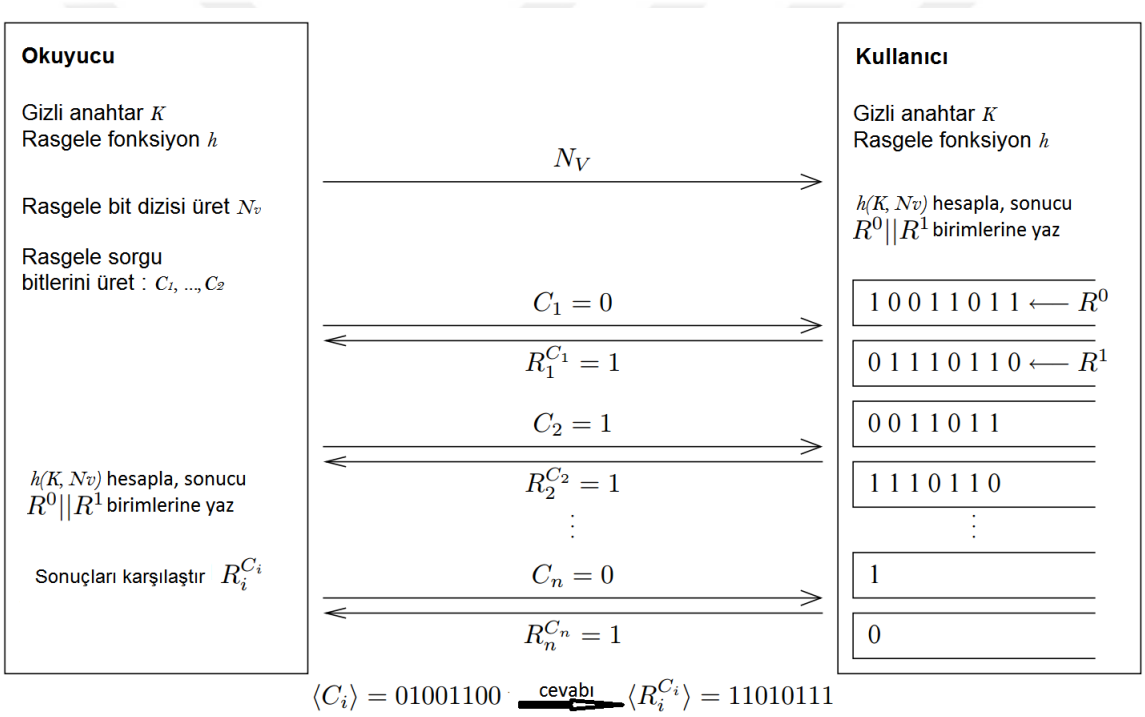
$$t_m = 2.t_p + t_d \tag{4.2}$$

Yukarıdaki denklemde t_d bir bitin işlem görmesi esnasında oluşan gecikmeler toplamıdır. İçerisinde kapı gecikmeleri, modemlerin modülasyon ve demodülasyon süreleri vardır. t_p elektromanyetik dalganın okuyucudan etikete ya da etiketten okuyucuya ulaşma süresidir. Elektromanyetik dalgalar hava içerisinde ışık hızına yakın hareket eder. Bu nedenle süresi mesafe ile orantılı şekilde değerler alır. Mesafe

ve gecikmeler arası ilişki aşağıdaki denklem ile bulunur. Buradaki c ışık hızını göstermektedir.

$$d = \frac{(t_m - t_d)c}{2} \tag{4.3}$$

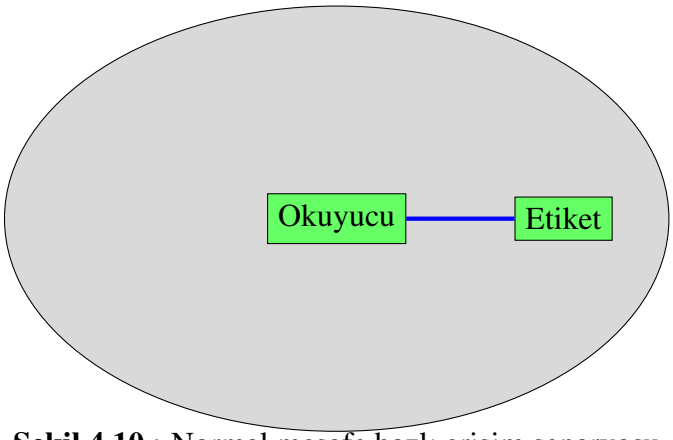
Okuyucu, etikete tek kullanımlık rastgele üretilen bir N_V bit dizisi gönderir. Etiket de okuyucuya tek kullanımlık bir rastgele bit dizisi N_P gönderir. Okuyucu ve etiket ortak sahip oldukları anahtar x'i ve tek kullanımlık oluşturulan N_V ve N_P bit dizisini özet (hash) fonksiyonuna gönderir. Fonksiyon $2n$ elemanlı bir bit dizisi çevrimi oluşturur. Sonuç olarak hesaplanan $2n$ elemanlı bit dizisi y_0 ve y_1 adında eşit sayıda eleman içeren iki alt diziye ayrılır.



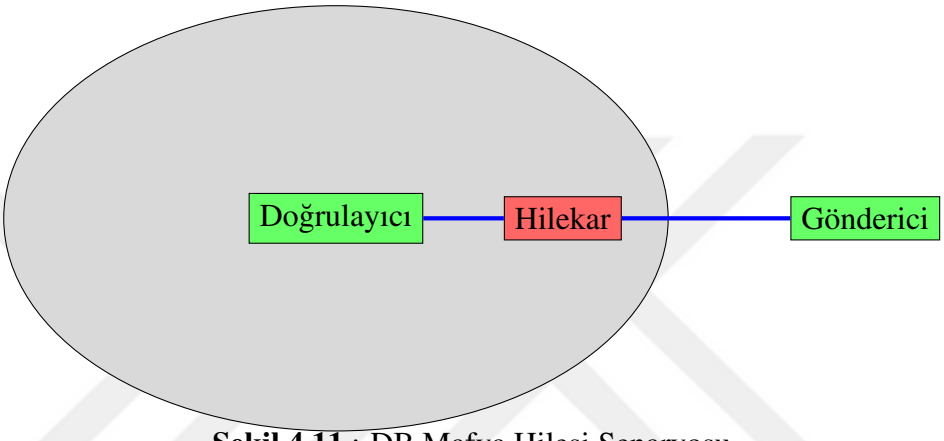
Şekil 4.9 : Hancke Kuhn Protokolü [2]

Bu işlemin ardından okuyucu n boyutlu tahmin edilemeyen rastgele oluşturulan bir C (sorgu) bit dizisi oluşturur. C dizisinin her elemanı sırayla etikete gönderilir. Etiket, gelen sorgunun değeri 1 ise y_1 bit dizisinden, 0 ise y_0 bit dizisinden bir bitlik yanıtlar gönderir.

Okuyucudan her gönderilen C_i sorgu bitine karşı etiketten gönderilen r_i cevap bitinin okuyucuya ulaşma gecikmesi Δt_i olarak belirlendikten sonra, bu değeri gerekli haberleşme hata hesaplamaları yapılıp belirlenmiş olan t_{max} ile karşılaştırarak etiketin sisteme giriş için uygun erişim bölgesinde olup olmadığı belirlenir. Mesafe tespitinden



Şekil 4.10 : Normal mesafe bazlı erişim senaryosu



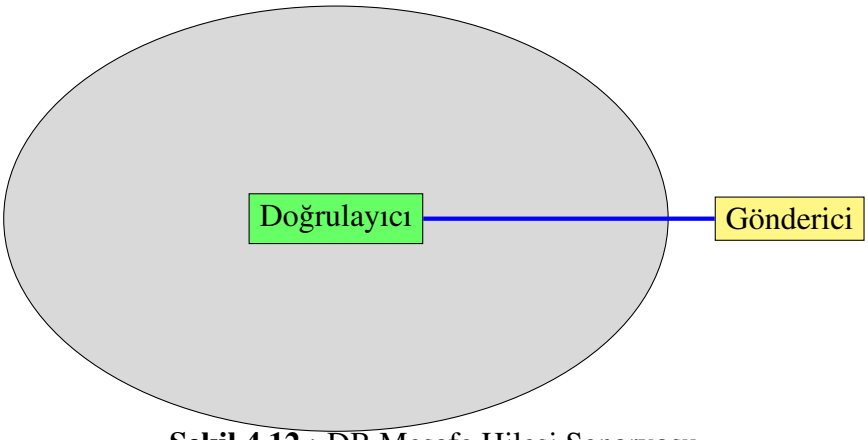
Şekil 4.11 : DB Mafya Hilesi Senaryosu

sonra ise alınan cevap bit dizisi ile olması gereken cevap bit dizisi karşılaştırılır. Okuyucu doğru cevapların sayısını eşik değerine göre kıyaslar ve etikete izin verir ya da erişimi iptal eder [2].

Normal şartlarda sistem erişimine ait dürüst kişi Şekil 4.10'da görüldüğü gibi sistem erişimi için yasal bölge içerisinden kendi etiketini kullanarak geçiş yapar. Buradaki senaryoya uyarlanabilecek mafya, terörist ve mesafe hilesi olarak adlandırılan 3 çeşit atak türü vardır [32].

4.2.6.2 Mafya Hilesi

Bu atak çeşidinde kötü niyetli kullanıcıya ait bir okuyucu-etiket sistemi bulunur. Burada hilekar Şekil 2.2'de görüldüğü gibi geçiş bölgesindedir. Geçiş bölgesinde olmayan sistem erişimine ait dürüst sistem kullanıcısının bilgileri ile o kişinin yerine geçerek sisteme erişimi olan dürüst kullanıcıymış gibi görünür. Gerçek sistem okuyucusu etiketin kimliğini sorgular, kötü niyetli kullanıcı aynı sorguyu kendi okuyucusuyla gerçek etikete gönderir. Etiket her hâlükârda sorguya uygun cevap



Şekil 4.12 : DB Mesafe Hilesi Senaryosu

verir, arada saldırgan olup olmadığını anlayamaz. Kötü niyetli kullanıcı, etiketten dönen cevabı aynı şekilde gerçek okuyucuya kendi etiketi ile gönderir ve bu döngüyü kullanarak sisteme erişim sağlamaya çalışır.

4.2.6.3 Mesafe Hilesi

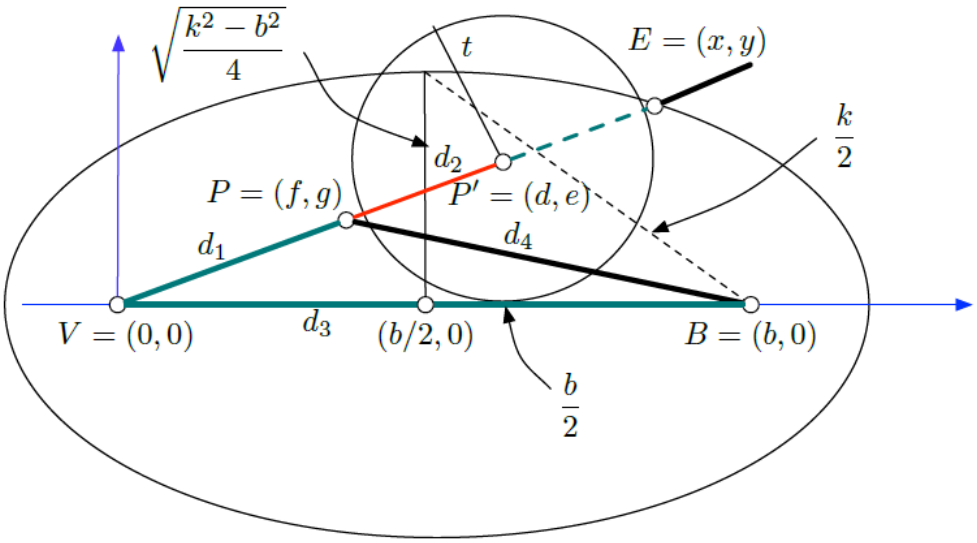
Bu atakta sistem erişimine ait dürüst olmayan kişi, Şekil 2.4'de görüldüğü gibi yasal erişim bölgesinde olmadığı halde okuyucuyu ilgili bölgedeymiş gibi yanıltarak sisteme erişim sağlamaya çalışır.

Daha uzakta olma atağını engellemek yani ADS-B sistemin güvenliğini arttırmak amacıyla tüm protokol tamamlandıktan sonra Şekil 4.13'da görüldüğü gibi alıcı istasyon ortak bir komşu seçer (B). Hem alıcının hem de kullanıcının komşusu olan B, TDOA yöntemiyle kullanıcının konum kestirimini verir. Hata eşik değerini aşan durumlarda B kullanıcının mesafesini daha uzakta gösterdiğini bilir.

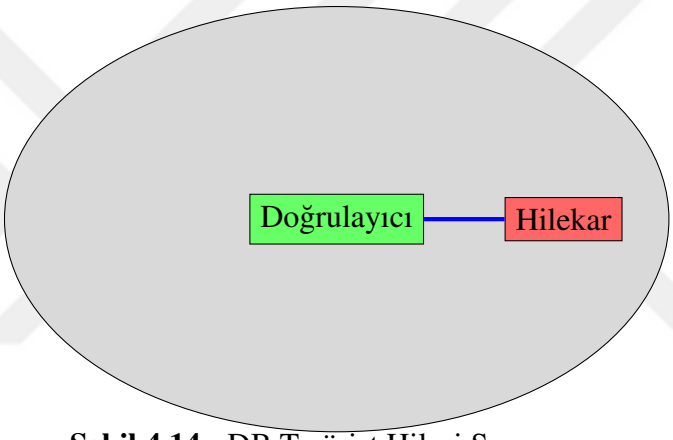
4.2.6.4 Terörist Hilesi

Sistem erişimine sahip ve dürüst olmayan kişi ile hilekar anlaşma yapar. Bu anlaşmada sistem erişimine sahip dürüst olmayan kişi sonraki erişimler için hiçbir ipucu içermeyecek şekilde sistemle ilgili, tek bir erişim için bilgiler verir. Burada sistem için gizli kalması gereken anahtar ile ilgili tek bir bit bile sızdıramamaktadır. Bu anlaşma sonrasında düşman Şekil 4.14'deki gibi erişim bölgesi içerisinde, sistem erişimine ait dürüst olmayan kişiden edindiği bilgiler ile sisteme giriş yapmaya çalışır.

Bahsedilen hilelerin konum tespitinin doğruluğu ve güvenliği için risk oluşturmaktadır. Mafya hilesi durumunda, saldırgan, meşru bir uçak ile doğrulayıcı arasında ölçülen mesafeyi kısaltabilir. Bununla birlikte, saldırgan, okuyucu ile sahte bir ADS-B



Şekil 4.13 : Mesafe Bazlı Protokol Şeması.



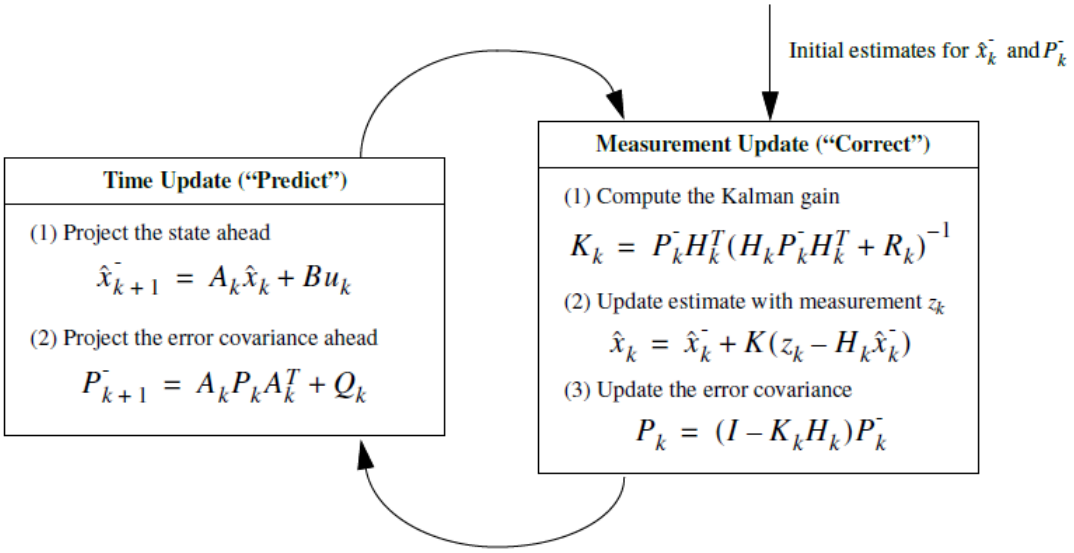
Şekil 4.14 : DB Terörist Hilesi Senaryosu

katılımcısı arasındaki ölçülen mesafeyi de kısaltabilir. Saldırganın mesafeyi kısaltabilmesi için saldırganla doğrulayıcı arasındaki fiziksel mesafenin kısa olması gerekmektedir. İşbirliği yapan doğrulayıcılardan da yararlanıldığında saldırının karmaşıklığını büyük ölçüde artırmaktadır. Özellikle mesafe sınırlaması diğer doğrulama teknikleriyle birleştirildiğinde, güvenilir bir uçuş yolunu taklit etmeyi zorlaştıracaktır. ADS-B bağlamında yalnızca mesafe hilesi tehlike olarak dikkate alınmalıdır. Bununla birlikte, gerekli zamanlama hassasiyeti, özellikle birden fazla doğrulayıcı bir araya getirildiği durumlarda saldırının başarılı olma yöntemini çok karmaşık hale getirir.

4.2.7 Kalman Filtresi Yöntemi

Durum uzayı modeli ile gösterilen bir dinamik sistemde, modelin önceki bilgileriyle birlikte giriş ve çıkış bilgilerinden sistemin durumlarını tahmin edilebilen filtredir.

Kalman Filtresi, 1960'lardan sonra araç navigasyonu başta olmak üzere (havacılık tipik olmasına rağmen başka uygulama alanları da vardır) kullanılan, sistemin durumu hakkında optimize edilmiş bir tahmin sağlayan bir algoritmadır. Algoritma, gürültülü, girdi gözlem veri akımları (tipik olarak, sensör (algılayıcı) ölçümleri) üzerinde özyinelemeli (recursive) olarak gerçek zamanlı çalışarak hataları en az-kareler eğriye sığdırma yöntemi ile filtre eder ve sistemin fiziksel karakteristiklerinin modellenmesi ile üretilen gelecek durumun matematiksel tahminine göre optimize eder [33].



Şekil 4.15 : Kalman Filtre Şeması.

Hava aracına pozisyon tahminini birkaç metre ile sağlayabilen bir GPS birimi takılabilir. GPS tahminleri gürültülüdür; okumalar, her zaman gerçek pozisyonun birkaç metre yakınında olmasına rağmen, hızlıca etrafta zıplayabilir. Hava aracının pozisyonu, manevraları ve dönüş açısını izleyerek, hızı ve yönü zamana göre entegre ederek de tahmin edilebilir. Bu teknik parakete hesabı olarak bilinir. Tipik olarak, parakete hesabı hava aracının yeri hakkında çok yumuşak bir tahmin sağlayacaktır, ancak küçük hatalar biriktikçe sapacaktır. Ayrıca, hava aracının fizik kurallarını takip etmesi de beklenir, yani pozisyonunun hızıyla orantılı olarak değişmesi beklenir. GPS hatalarını düzeltmek amacıyla ADS-B protokolüne Kalman Filtresi yöntemi adapte edilebilir [33].

4.3 Analiz

Çizelge 4.1 ve 4.2'de önerilen atak çeşitleriyle mücadelede incelenen bütün çözümlerin üstünlüğü ve fizibilite ile ilgili dezavantaj ve avantajlara değinerek kompakt bir genel

Çizelge 4.1 : Güvenlik özellikleri

Güvenlik Tipi	Veri Bütünlüğü	Kaynak Bütünlüğü	Konum Doğrulama	DoS
Makine Öğrenmesi	Yok	Var	Yok	Kısmen
Eşgüdümsüz Frekans Atlamalı Yöntem	Yok	Yok	Yok	Var
Kriptografik Yöntemler	Var	Var	Var	Kısmen
Geriye Dönük Anahtar Yayınlama Yöntemi	Yok	Var	Yok	Yok
Çoklu Algılama ve Konumlama Yöntemi	Yok	Yok	Var	Yok
Mesafe Bazlı Protokoller	Yok	Yok	Kısmen	Yok
Kalman Filtreleme	Yok	Kısmen	Kısmen	Yok

bakış sunmaktadır. Tasarlandığı gibi, halen kullanımda olan ADS-B yazılımı ve donanımı üzerinde çok az etkisi olan çözümler göz önüne alındığında, tek bir optimum çözüm bulunmamaktadır. Çizelge 4.1, tartışılan yaklaşımların karşı koyabileceği güvenlik ihlallerini göstermektedir. ADS-B protokolünün açık mesajlaşma yapısı çoğu senaryoda kötü niyetli bireylerin kullandığı bir özellik olarak düşünülmüştür. Dolayısıyla, hava trafiği iletişimi ve kontrolünün ele alınma biçiminde büyük bir paradigma değişikliği olmadıkça, daha sofistike ve sorunlu saldırılar için olması yüksek ihtimal dahilindedir. Pasif dinleyicilere karşı koruma konusunda herhangi bir gelişim yoktur. Protokolde baştan aşağı bir şifreleme çözümü olmadan pasif dinleme ataklarına karşı korumak çok zordur. Tartışılan tüm yaklaşımlar, doğrulama yoluyla (kriptografik yöntemler) ya da verilerdeki anormallikleri tespit ederek (örn. Kalman filtrelemesi, çok alıcılı sistem) doğrudan mesajın eklenmesi ve değiştirilmesine değinir.

Çizelge 4.1'de güvenlik planlarının sağlayabileceği güvenlik özelliklerine değinilmiştir. Daha önce de bahsedildiği gibi kriptografik açık anahtar altyapısı, alınan verilerin yalnızca bütünlüğünü garanti eder. Diğer tüm yaklaşımlar kaynağın bütünlüğünü sağlamayı veya sağlanan konum verilerini bağımsız olarak doğrulamayı amaçlamaktadır. ATC sistemlerine karşı sinyal engelleme saldırılarına karşı önlemler, yayılmış spektrum yaklaşımları ve kriptografi ile doğrudan sağlanabilirken, diğer yöntemler meşru uçak girişlerini tespit etmek için üst katmanlarda önlem alınır.

Çizelge 4.2'de, özellikle havacılık endüstrisinde hava trafik kontrolünün mevcut durumu göz önüne alarak, pratik uygulamalardaki farklı yaklaşımların fizibilitesine

Çizelge 4.2 : Fizibilite özellikleri

Güvenlik Tipi	Zorluk	Masraf	Ölçeklenebilirlik	Uygunluk
Makine Öğrenmesi	Değişken	Değişken	Değişken	Ek donanıma ve yazılıma ihtiyaç vardır. ADS-B protokolünde değişikliğe sebep olmaz
Eşgüdümsüz Frekans Atlamalı Yöntem	Orta	Orta	Orta	Yeni donanım ve yeni fiziksel katman gerektirir
Kriptografik Yöntemler	Yüksek	Yüksek	Orta	Dağıtım altyapısı ve ADS-B protokolündeki değişiklik gerektirir
Geriye Dönük Anahtar Yayınlama Yöntemi	Orta	Orta	Yüksek	Anahtar yayını için yeni ileti türü (MAC) gerektirir
Çoklu Algılama ve Konumlama Yöntemi	Düşiük	Orta	Orta	ADS-B'de değişiklik gerektirmez. Ayrı donanım sistemi gerektirir
Mesafe Bazlı Protokoller	Yüksek	Orta	Düşük	Yeni bir mesajlaşma protokolü gerektirir
Kalman Filtreleme	Yok	Kısmen	Kısmen	Ayrı bir yazılıma gerektirir

genel bir bakış sunmaktadır. Tahmin edileceği gibi zorluk ve maliyet sütunları çoğunlukla birbiriyle ilişkilidir. Geniş alanlı çoklu alıcılı yöntem ve Kalman filtreleri halihazırda kullanımdadır. Bu yöntemlerin uygulaması, doğal olarak, endüstri kararlarında önemli bir rol oynayan maliyet faktörüne dönüşür. NextGen'e tamamen geçiş yapılana kadar çeşitli ATC sistemlerinin ve verilerin (PSR, SSR, ADS-C, WAMLAT, FANS) kaynaştırılması gereklidir. Yine de, havacılık camiasında, "Otomatik Bağımlı Gözetim, konvansiyonel radar sistemlerine bağımlılığın kaldırılması veya azaltılması nedeniyle oluşan tasarruflara atfedildiği" düşüncesi yaygındır. Bu nedenle, başlangıçta ADS-B'nin güvenlikle ilgili yetersizliğini gidermek için, geniş ölçekte ilkel radar sistemlerine sahip olmak gerekmektedir.

5. SONUÇ VE ÖNERİLER

Çeşitli kaynaklardan gelen verileri bir araya getirme gibi diğer teknikler, ATC tarafından elle yapılmaktadır. Olağandışı ADS-B verileri görüldüğünde, radar ve uçuş planı verileri gibi diğer kaynaklar da elle kontrol edilir. Literatürde, ADS-B'nin ilkel radar sistemlerinin yerini alacağı izlenimi verilirken, trafik yoğunluğuna ve iyi bir altyapıya sahip Avrupa kıtası gibi bölgeler gelecekte de birincil radar tarafından karşılanmaya devam edecektir.

Bununla birlikte, sahte uçakların sayısı arttıkça kontrolörlerin iş yükü artacaktır. Dahası, meşru bir uçağın daha önce uçtuğu yolu tekrar tekrar oynatmak maliyetli olacaktır. Bu sorunun üstesinden gelmek için, radar verileri, ADS-B ve uçuş planı verileriyle otomatik olarak senkronize edilmesi gerekmektedir. İlkel radar sistemlerinin uygulanabilir bir seçenek olmadığı alanlarda çok alıcılı yöntem, veri füzyonu sistemine bağlanabilir. Sahte ADS-B sinyalleri, hava trafik kontrolörlerinin ekranlarında işaretlenecek ve hava trafik kontrolörlerinin ekranlarından çıkarılacaktır. Bu alanlarda kullanılabilecek bir diğer yöntem de Kalman filtrelemedir. Bu sayede belirli bir uçak türü muhtemelen yapamayacağı bir manevra oluşturduğunda meşru sinyal olduğu tespit edilir. Ancak bu teknik, bir talebinin orijinal olup olmadığını belirlemek için yüzde yüz güvenilir değildir.

Bu çalışamada ADS-B'ye yönelik ataklar okuyucuya aktarılmış ve güvenliğini arttırmaya yönelik algoritmalar ve yöntemler tanıtılmış, bu metodların uygulanabilirliği hakkında bilgiler verilmiştir. Siber güvenlik tehditlerinin çokça arttığı bu dönemde, uluslararası havacılık teknolojisinde uçak ve kule haberleşmesini sağlayan ADS-B mesajarında uçuş bilgilerinin şifrelenmemiş sinyal üzerinden yayılması gibi açık noktaların var olması büyük bir endişe kaynağıdır. Gelecek çalışmalarda, ADS-B sinyallerinin uygulanabilirliği ve sağladığı güvenlik açısından, asimetrik açık anahtar şifreleme metoduylarıyla gerçeklenmesi sağlanacaktır.

KAYNAKLAR

[1] **Mozdzanowska, A.L.**, **Weibel, R.E. ve Hansman, R.J.** (2008). Feedback model of air transportation system change: Implementation challenges for aviation information systems, *Proceedings of the IEEE*, *96*(12), 1976–1991.

[2] **Hancke, G.P. ve Kuhn, M.G.** (2005). An RFID distance bounding protocol, *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, IEEE, s.67–73.

[3] **Planning, J.** *ve diğerleri*, (2007), Concept of operations for the next generation air transportation system.

[4] **FAA**, NextGen Implementation Plan, `https://www.faa.gov/nextgen/media/NextGen_Implementation_Plan-2016.pdf`, alındığı tarih: 10.04.2017.

[5] **Kazda, A. ve Caves, R.E.** (2010). *Airport design and operation*, Emerald Group Publishing Limited.

[6] **FAA**, 2025. Washington, DC: Federal Aviation Administration, US Department of Transportation (Aug 2011).

[7] **Law, J.**, Cascade News 7, `http://www.ssd.dhmi.gov.tr/getBinaryFile.aspx?Type=3&dosyaID=201`, alındığı tarih: 10.01.2017.

[8] **Atanasov, A. ve Chenane, R.** (2013). Security Vulnerabilities in Next Generation Air Transportation System.

[9] **Cir, I.** 319, 2009. A Unified Framework for Collision Risk Modelling in Support of the Manual on Airspace Planning Methodology for the Determination of Separation Minima (Doc. 9689), *International Civil Aviation Organization, Montreal, Canada*.

[10] **Galotti, V.** (1997). *The Future Air Navigation System (FANS)*.

[11] **ICAO** (2000). National Plan for CNS/ATM Systems.

[12] **Hamit, S.** (2016). ATS gözetim sistemleri ve hizmetleri, DHMİ, s.83–97.

[13] **Stevens, M.C.** (1988). *Secondary surveillance radar*, Artech House on Demand.

[14] **Trim, R.** (1990). Mode S: an introduction and overview (secondary surveillance radar), *Electronics & Communication Engineering Journal*, *2*(2), 53–59.

[15] **Bruno, R. ve Dyer, G.** (2008). Engineering a US national Automatic Dependent Surveillance-Broadcast (ADS-B) radio frequency solution, *Digital Communications-Enhanced Surveillance of Aircraft and Vehicles, 2008. TIWDC/ESAV 2008. Tyrrhenian International Workshop on*, IEEE, s.1–6.

[16] **Billaud, P.**, **De Volder, C. ve Wybierala, M.**, (1994), Method and device to detect the garbling of pulses received by a secondary radar, uS Patent 5,341,139.

[17] **Ali, B.** (2013). A Safety Assessment Framework for Automatic Dependent Surveillance Broadcast (ADS-B) and its Potential Impact on Aviation Safety, *Doktora Tezi*, Imperial College London.

[18] **Sun, J.** (2017). ADS-B Decoding Guide.

[19] **GAO** (2002). Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed.

[20] **Sampigethaya, K. ve Poovendran, R.** (2011). Security and privacy of future aircraft wireless communications with offboard systems, *Communication Systems and Networks (COMSNETS), 2011 Third International Conference on*, IEEE, s.1–6.

[21] **Costin, A. ve Francillon, A.** (2012). Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices, *Black Hat USA*, 1–12.

[22] **Li, W. ve Kamal, P.** (2011). Integrated aviation security for defense-in-depth of next generation air transportation system, *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, IEEE, s.136–142.

[23] **Sampigethaya, K. ve Poovendran, R.** (2009). Privacy of future air traffic management broadcasts, *Digital Avionics Systems Conference, 2009. DASC'09. IEEE/AIAA 28th*, IEEE, s.6–A.

[24] **RTCA** (2002). *Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B).*, RTCA, Incorporated.

[25] **Strohmeier, M.**, **Lenders, V. ve Martinovic, I.** (2015). On the security of the automatic dependent surveillance-broadcast protocol, *IEEE Communications Surveys & Tutorials*, *17*(2), 1066–1087.

[26] **Strasser, M.**, **Pöpper, C.**, **Capkun, S. ve Cagalj, M.** (2008). Jamming-resistant key establishment using uncoordinated frequency hopping, *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, IEEE, s.64–78.

[27] **Zhang, J. ve Varadharajan, V.** (2010). Wireless sensor network key management survey and taxonomy, *Journal of Network and Computer Applications*, *33*(2), 63–75.

[28] **Feng, Z.**, **Pan, W. ve Wang, Y.** (2010). A data authentication solution of ads-b system based on x. 509 certificate, *27th International Congress of the Aeronautical Sciences, ICAS*, s.1–6.

[29] **Perrig, A.**, **Canetti, R.**, **Tygar, J.D. ve Song, D.** (2005). The TESLA broadcast authentication protocol, *Rsa Cryptobytes*, *5*.

[30] **Miyazaki, H.**, **Koga, T.**, **Ueda, E.**, **Yamada, I.**, **Kakubari, Y. ve Nihei, S.** (2009). Evaluation results of multilateration at narita international airport, *Proc. Inter. Association of Institute of Navigation (13th IAINWorld Congress)*.

[31] **Brands, S. ve Chaum, D.** (1993). Distance-bounding protocols, *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, s.344–359.

[32] **Kocaağa, E.**, **Tanıl, B.**, **Bingöl, M.A. ve Kardaş, S.** (2013). Solution of a Conjecture: On 2-PCD RFID Distance Bounding Protocols, *ISC Turkey*.

[33] **Da Silva, J.L.**, **Brancalion, J.F. ve Fernandes, D.** (2009). Data fusion techniques applied to scenarios including ADS-B and radar sensors for air traffic control, *Information Fusion, 2009. FUSION'09. 12th International Conference on*, IEEE, s.1481–1488.

ÖZGEÇMİŞ

Ad Soyad:Eren Kocaağa

Doğum Tarihi ve Yeri:31.10.1992 Antalya

E-Posta:kocaagae@itu.edu.tr

ÖĞRENİM DURUMU:

- **Lisans:** 2015, İstanbul Teknik Üniversitesi, Elektrik Elektronik Fakültesi, Elektronik ve Haberleşme Mühendisliği
- **Y. Lisans:** 2017, İstanbul Teknik Üniversitesi, Bilişim Enstitüsü, Bilgi Güvenliği Mühendisliği ve Kriptografi.

MESLEKİ DENEYİMLER VE ÖDÜLLER:

- 2016 yılından itibaren TÜBİTAK BİLGEM Bİlişim Teknolojileri Enstitüsü'nde Araştırmacı olarak çalışmaktadır.
- 2014–2016 yılları arasında İstanbul Teknik Üniversitesi ARI 2 Teknokent'te bulunan ERLAB firmasında Yazılımcı olarak çalışmıştır.
- 2013 yılında 2,5 ay TURKCELL'de ICT ERP uzun dönem Stajyer olarak çalışmıştır.
- 2013 yılında 1 ay TÜBİTAK BİLGEM'de Stajyer olarak çalışmıştır.
- 2012 yılında 1 ay DHMİ Antalya'da Stajyer olarak çalışmıştır.

YÜKSEK LİSANS TEZİNDEN TÜRETİLEN YAYINLAR SUNUMLAR VE PATENTLER:

- Külekci O.,Kocaağa E., 2017. Otomatik Bağımlı Gözetim Yayını Güvenlik Analizi. *SIU 2017*, Mayıs 15-18, 2017 Antalya, Turkey. (Sunum ve bildiri örneği)