
GAZİ ÜNİVERSİTESİ
Gazi
1926

İNSANSIZ HAVA ARACI SİSTEMLERİNDE BİLGİ GÜVENLİĞİ VE RİSK TABANLI ÇOK KRİTERLİ KARAR VERME MODELİ İLE DEĞERLENDİRİLMESİ

İsmet ÇUHADAR

DOKTORA TEZİ

KAZALARIN ÇEVRESEL VE TEKNİK ARAŞTIRMASI ANABİLİM DALI

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

EYLÜL 2017

İsmet ÇUHADAR tarafından hazırlanan "İNSANSIZ HAVA ARACI SİSTEMLERİNDE BİLGİ GÜVENLİĞİ VE RİSK TABANLI ÇOK KRİTERLİ KARAR VERME MODELİ İLE DEĞERLENDİRİLMESİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Kazaların Çevresel ve Teknik Araştırması Anabilim Dalında DOKTORA TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Mahir DURSUN

Elektrik-Elektronik Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum. .....

Başkan: Prof. Dr. Kemal LEBLEBİCİOĞLU

Elektrik-Elektronik Mühendisliği Anabilim Dalı, ODTÜ

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum. .....

Üye: Prof. Dr. Mustafa ALKAN

Elektrik-Elektronik Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum. .....

Üye: Prof. Dr. M. Ali AKÇAYOL

Bilgisayar Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum. .....

Üye: Doç. Dr. Uğur ÖZCAN

Endüstri Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum. .....

Tez Savunma Tarihi: 26/09/2017

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

.....

Prof. Dr. Hadi GÖKÇEN

Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

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

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

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

İsmet ÇUHADAR

26/09/2017

İNSANSIZ HAVA ARACI SİSTEMLERİNDE BİLGİ GÜVENLİĞİ VE RİSK TABANLI ÇOK KRİTERLİ KARAR VERME MODELİ İLE DEĞERLENDİRİLMESİ

(Doktora Tezi)

İsmet ÇUHADAR

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Eylül 2017

ÖZET

Teknolojinin gelişmesiyle birlikte, İHA kullanımı her geçen gün artmaktadır. Bu artışa paralel olarak kullanım alanları da; keşif/gözetleme desteği, taarruz elektronik harp, hedef benzetimi, özel/spesifik görevler gibi askeri amaçların yanı sıra atmosfer gözlemleme, hava tahmini ya da bilimsel araştırma, boru hatları takibi, yol kontrolü, arama ve kurtarma çalışmaları, hava fotoğrafçılığı, petrol, gaz ve mineral araştırmaları gibi sivil sahalarda da yaygınlaşmıştır. İHA sayısının artması, iyi maksatlı kullanımla birlikte kötü niyetli kullanımları da gün yüzüne çıkarmış ve günümüzde kötü amaçlı İHA kullanımı büyük bir tehdit haline gelmiştir. Bu tehdit, doğrudan temin edilen İHA'lar ile yapılabileceği gibi kontrolü ele geçirilen İHA'lar ile de sağlanabilmektedir. Bu insansız sistemlerin saldırıya karşı en zayıf alt sistemi haberleşmedir. Uzun mesafelerde veri iletimi yanında, doğru noktaya doğru bilgi göndermek büyük önem taşımaktadır. Haberleşme, elektronik harp ve siber saldırı yöntemleri ile ele geçirilebilmekte veya yanıltılabilmektedir. Bu çalışmada önerilen yöntem ile İHA'ların ele geçirilmesi, yöneltilmesi ve yanıltılması gibi kötü maksatlı istismarlara karşı tedbir getirilmesi ve yöntemin Risk Tabanlı Çok Kriterli Karar Verme ile değerlendirilmesi hedeflenmiştir.

Bilim Kodu : 90611
Anahtar Kelimeler : İHA, haberleşme, veri linki güvenliği, kriptolama, risk analizi.
Sayfa Adedi : 139
Danışman : Doç. Dr. Mahir DURSUN

UNMANNED AIR VEHICLE DATA LINK SAFETY AND EVALUATING WITH RISK BASED MULTI CRITERIA DECISION MAKING MODEL

(Ph.D. Thesis)

İsmet ÇUHADAR

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

September 2017

ABSTRACT

With the development of technology, UAV usage has been increasing day by day. In parallel with this increase, usage areas like reconnaissance/surveillance support, electronic warfare, target simulation, special/specific tasks, atmosphere monitoring, weather forecast or scientific research, pipeline tracking, path control, search and rescue operations, aerial photography, oil, gas and mineral research have also increased. The increasing number of UAV uncovered the malicious usage as much as well-purpose usage day by day and malicious usage of UAVs has become today a major threat. This threat can be achieved by both owned UAVs or captured UAVs. Communication is the most susceptible subsystem of the unmanned systems against attacks. Besides the transmission of data over long distances, to send the right information at the right point is of great importance. Communication subsystem can be seized or misled by electronic warfare and cyber-attack. With the method revealed in this study, it is aimed to introduce measures against bad intentional abuse like UAV seized, misled or feint. And it is also aimed to evaluate the method with Risk Based Multi Criteria Decision Making.

Science Code : 90611
Key Words : UAV, communications, data link security, encryption, risk analysis.
Page Number : 139
Supervisor : Associate Professor Mahir DURSUN

TEŞEKKÜR

Doktora eğitimime devam ettiğim beş yıl boyunca, kayıttan mezuniyete kadar tüm safhalarda, desteğini ve yardımını benden esirgemeyen Doç. Dr. Mahir DURSUN'a "Gazi Üniversitesi" şükranlarımı sunarım. Yeterlilik sınavını müteakip başladığım tez aşaması süresince beni ve çalışmalarımı sabırla takip eden ve doğru yönde uygun adımların atılmasını sağlayan Prof. Dr. Mustafa ALKAN "Gazi Üniversitesi" ve Prof. Dr. Mehmet Ali AKÇAYOL'a "Gazi Üniversitesi" müteşekkirim. Ayrıca, 2211-Yurt İçi Doktora Burs Programı kapsamında sağladığı destekten ötürü TÜBİTAK Bilim İnsanı Destekleme Daire Başkanlığı birimine teşekkür ederim. Son teşekkürüm de; hayatımın tamamı gibi doktora eğitimimi de zevkli hale getiren ve her türlü kaprisime katlanarak bana destek olan eşime; iyi ki varsın.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

SİMGELER VE KISALTMALAR

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

Simgeler	**Açıklamalar**
cm-hg	Santimetre civa
dB	Desibel
fps	Frame per second
Kb	Kilobayt
Kbps	Kilobayt/saniye
Km	Kilometre
m/s	Metre/saniye
Mb	Megabayt
Mbit/s	Megabit/saniye
MHz	Mega hertz
MHz	Giga hertz
µs	Mikro saniye

Kısaltmalar	**Açıklamalar**
AGL	Above ground level- yer seviyesine göre irtifa
AoA	Angle of arrival
AES	Advanced encryption standard
BLOS	Beyond line of sight
BTK	Bilgi Teknolojileri Kurumu
CA	Certificate Authority
CBC	Cipher block chaining
CEPT	Commission of European Post and Telecom
CFB	Cipher feedback
CSI	Camera Serial Interface
DARPA	Defense Advanced Research Projects Agency
DF	Direction finding

Kısaltmalar	Açıklamalar
ECB	Electronic code book
EH	Elektronik harp
EHK	Elektronik haberleşme kanunu
FAA	Federal Aviation Administration
GPS	Global positioning system
GNSS	Global navigation satellite system
HDMI	High Definition Multimedia Interface
HF	High frequency
HTTP	Hyper text transfer protocol
HTTP	Secure hyper text transfer protocol
ICAO	International Civil Aviation Organization
IEEE	Institute of Electric and Electronic Enginering
IEO	Information utility value oriented encryp. opt.
IMO	International Maritime Organization
IMU	Inertial measurement unit
ITU	International Telecommunication Union
IP	Internet Protocol
İHA	İnsansız hava aracı
İHAS	İnsansız hava aracı sistemi
J/N	Jamming to noise
JPEG	Joint Photographic Experts Group
KEGM	Kıyı Emniyeti Genel Müdürlüğü
KET	Kısa mesafe erişimli telsiz
KKO	Kriter karşılama oran
LAN	Local area network (Yerel alan ağı)
LOS	Line of sight
MIME	Multipurpose internet mail extensions
ML	Maximum likelihood
MLS	Method of least square
MUSIC	Multiple signal characterization
NN	Nearest neighbors
PEM	Privacy Enhanced Mail

Kısaltmalar	Açıklamalar
RF	Radyo frekans
RPV	Remote piloted vehicle
RR	Radio regulation
RSS	Received signal strength
RSSI	Received signal strength indicator
RTSP	Real time streaming protocol
SDHC	Secure digital high capacity
SİNİS	Sinyal istihbarat
SNR	Signal to noise ratio
SSL	Secure Socket Layer
SSM	Savunma Sanayi Müsteşarlığı
TCP	Transmission Control Protocol
TDoA	Time difference of arrival
TLS	Transport Layer Security
ToA	Time of arrival
UDP	User datagram protocol
URL	Uniform/universal resource locator
USRP	Universal software radio peripheral
VEA	Video encryption algorithm
VHF	Very high frequency
YKİ	Yer kontrol istasyonu
YVT	Yer veri terminali

1. GİRİŞ

Genel olarak bilinen adıyla drone uzaktan kumanda edilen bir tür uçaktır. Keşif amaçlı üretilen bu araçlar günümüzde birçok saldırı görevinde de kullanılmaktadır. Ayrıca, askeri amaçlar dışında; atmosfer gözlemleme, hava tahmini ya da bilimsel araştırma, boru hatları takibi, yol kontrolü, arama ve kurtarma çalışmaları, hava fotoğrafçılığı, petrol, gaz ve mineral araştırmaları, kargo/kurye hizmetleri gibi sivil sahalarda kullanılmaya başlanmıştır [1].

İlk İHA A.M. LOW tarafından 1916 yılında geliştirilmiştir. 1935 yılında ise model uçak tasarımcısı Reginald DENNY ilk ölçekli RPV (Remote Piloted Vehicle) modelini geliştirmiştir. Jet motoru bulunan ilk model İHA 1951 yılında Teledyne Ryan firması tarafından geliştirilen Firebee'dir. 1955 yılında ise başka bir firma Beechcraft ABD Deniz Kuvvetleri için Model 1001 tipini üretmiştir.

1980'li ve 1990'lı yıllarda riskli görevlere hazırlanan ABD ordusu uçakların kısa süreli havada kalabilmesi, alçaktan uçması ve çok ses yapması nedeniyle kolayca hedef haline gelmesi, havadan yapılan keşiflerin uçakların hızı nedeniyle çözünürlüğünün düşük süresinin az olması gibi sebeplerle İHA'lar karşısında ve küçültülen bu araçlar özellikle ABD'li askeri çevrelerin ilgisini çekmeye başlamıştır. Bunun en önemli nedeni İHA'ların uçaklara göre çok daha ucuz olması ayrıca riskli görevlerde sırasında yetişmiş mürettebat kaybını sıfıra indirmesidir. Genel olarak keşif ve gözetleme amacıyla kullanılan bu araçların son yıllarda silahlı olarak kullanımı da yaygınlaşmıştır.

Günümüzde birçok firma tarafından irili ufaklı İHAS üretilmektedir. İHA'ların hala en yaygın kullanım maksadının keşif ve gözetleme yani özünde bilgi edinme ve istihbarat olduğu düşünüldüğünde İHA'ların en kritik alt sisteminin haberleşme (veri linki) sistemi olduğu daha net olarak ortaya çıkmaktadır. İHA'ların yaygınlaşması, bilgi/veri linki güvenlik sorununun da önemini artırtışmış, güvenilir veri transferi ihtiyacı ile veri iletim yöntemleri hakkında soru işaretlerine neden olmuştur.

İHA'ların düşük maliyetlerle ve kolayca elde edilmesi nedeniyle güvenilirliklerinin de sorgulanırlığını artmıştır. İHA'ların kendilerinin saldırı aracı olarak kullanılabileceği gibi,

İHA'ların kendilerine de saldırılması sıkça karşılan bir olay haline gelmiştir. Bu nedenle hava araçlarının sağlam ve güvenilir olması önem arz etmektedir. Bu maksada ulaşılabilmesi için ilk ele alınması ve geliştirilmesi gereken husus İHA'larda veri linkidir. İHA'lar birçok firma tarafından üretilmekle birlikte, veri linki/iletişim güvenlik sorunu halen devam etmektedir. Uzun mesafelere veri iletiminin yanı sıra doğru bilgiyi doğru noktaya göndermek büyük önem taşımaktadır. Arıca veri iletiminde sıkça yaşanan dış müdahalelere de engel olunması gerekmektedir.

Sonuç olarak; veri linkine dışardan müdahalenin önlenmesi ve uzun mesafelerde veri iletiminde doğru bilginin doğru noktaya gönderilebilmesi maksadıyla güvenli görüntü/veri aktarım yönteminin geliştirilmesi önem arz etmektedir. Bu çerçevede yapılan araştırmanın amacı; İHA sistemlerinde kablosuz veri linklerinin (aşağı/yukarı) tüm yönleri ile (güçlü ve zayıf) incelenerek dışardan müdahalenin önlenmesi ve uzun mesafelerde veri iletiminin doğru ve güvenilir bir şekilde yapılabilmesi maksadıyla güvenli görüntü/veri aktarım yöntemini geliştirmek ve bu hususta milli yeteneklere sahip olmaktır.

Tüm bu hususlar kapsamında projenin önemi; Türkiye'de yeni gelişmekte olan bir sektörde/alandaki önemli bir açığı gidererek İHA sistem tasarım ve geliştirme sürecine girdi sağlanacak olması, ileride meydana gelebilecek bilgi güvenliği açıklarının engellenecek/oranın azaltılacak olması ve nihayetinde de ülkemizin bu sektörde söz sahibi bir konuma gelmesinden kaynaklanmaktadır. İHA'nın özellikle ülkemizde yeni gelişmekte ve üretilmekte olması, ayrıca İHAS kullanıcılarının Türk Silahlı Kuvvetleri ve Emniyet Genel Müdürlüğü gibi özel kamu kurumları olması nedeniyle İHA üretimine ilişkin net bilgilere ve ilgili şahıs/kurum/kuruluşlara ulaşılmasındaki güçlükler tez çalışması süresince sıkıntılara neden olmuştur.

Çalışmamızda, İHA sistemlerinde veri linki güvenliği sorununa bir çözüm bulmak için İHA ve yer kontrol istasyonu arasında karşılıklı olarak görüntülerin ve verilerin güvenli bir şekilde aktarılmasını sağlayacak bir yöntem üzerinde durulmuştur. Güvenli görüntü aktarımı için yeni bir şifreleme yöntemi geliştirilmemiş ancak var olan farklı yöntemler farklı bir alan olan İHA sistemlerine uyarlanarak ve birlikte kullanılarak alternatif bir yöntem geliştirilmiştir. Bu yolla, Motion-Jpeg, TCP/IP, TLS/SSL ve kullanıcı kimlik doğrulama/yetkilendirme sistemi ile dört adımlı bir güvenlik sistemi önerilmiştir. Sonuç olarak, bu düşük maliyetli, güvenilir, yönetilebilir, güvenli ve uygulanabilir yöntemde,

veriler Raspberry Pi 3 ve Picamera modülü kullanılarak Go Language ile yazılan kod vasıtası ile HTTPS üzerinden aktarılmış ve yöntem ayrıca deneyle de doğrulanmıştır.

Dijital kameralar, IP kameralar ve web kameraları gibi video yakalama cihazları tarafından yaygın olarak kullanılması, video akışında meydana gelen hızlı değişimleri kolayca tolere edebilmesi, Safari, Google Chrome, Mozilla Firefox ve Microsoft Edge gibi web tarayıcılar tarafından desteklenmesi, nedenleri ile Motion-JPEG formatının kullanılmasını tercih edilmiştir. HTTP desteği, bağlantı odaklı olması, yüksek güvenilirlik gerektiren uygulamalar için uygun olması, verilerin bozulmadan ve gönderildiği sırayla gideceği garantisi, üç yönlü el sıkışma ile Akış Kontrolü ve Hata Kontrolü/Düzeltme yapması gibi avantajlara sahip olması nedeniyle de IP trafiği olarak TCP kullanılmıştır. Sertifika ve anahtara dayalı şifreli kanal oluşturduğu, daha çok veriyi daha kısa sürede şifreleyerek aktarabildiği, bu maksatla hava aracı üzerinde ilave donanım ihtiyacı gerektirmediği, aynı zamanda iki yönlü veri akışı güvenli olarak sağlayabildiği, hem telemetre (komut ve rapor) hem de video gibi veriler eş zamanlı olarak gönderilebildiği için TLS protokolünün kullanılması tercih edilmiştir.

Yazılımda yapılan bir geliştirme ile görüntü aktarımı etkinleştirilmiş ve hızlandırılmıştır. Bu kapsamında; aynı resmin birden fazla gönderilmesi engellenmiş, böylece aktarılan resim sayısı ve paralelinde veri trafiği de benzer şekilde azaltılmış, CPU kullanımı ve paralelinde ihtiyaç duyulan donanım özelikleri düşürülmüştür.

Şifreli kanala giriş ve çıkışlarında güvenli olması için bir arayüz ile kullanıcı giriş sistemi oluşturulmuştur. Kullanıcıların tüm bağlantıları kayıt altına alınmaktadır. Kullanıcı adı ve şifresinin güvenli kanal (TLS) üzerinden şifrelenerek gönderilmesi, böylece istenmeyen kişilerce (eavesdropping) elde edilememesi amaçlanmıştır.

Yapılan literatür taraması kapsamında; Qiao Lintian ve Nahrsîedt Klara 1997 yılında yaptıkları bir çalışma ile önce sıkıştırılmış video verilerinin istatistiksel karakterini incelemişler ve sıkıştırma işleminden dolayı byte seviyesinde rastsallığın fazla olduğu sonucuna ulaşmış olduklarını belirtmişler ve bu sonuca uygun olarak Video Şifreleme Algoritmasını (Video Encryption Algorithm-VEA) önermişlerdir. Bu algoritma kapsamında; şifrelenmemiş veri tek-çift bitler olarak iki gruba ayrılmakta, tekli grup şifrelenmiş ve şifrelenmiş olan bu tekli grup ile şifrelenmemiş çiftli grup birleştirilerek yeni bir grup oluşturulmuştur [2].

Wander Arvinderpal S., Gura Nils, Eberle Hans, Gupta Vipul, Shantz Sheueling Chang ise 2005 yılındaki çalışmalarında; RSA ve eliptik eğriler yönteminin asimetrik kripto sisteminde yaygın olarak kullanıldığını, eliptik eğriler yönteminin RSA kadar ilgi çektiğini ancak daha küçük anahtara sahip olduğunu ileri sürmüş, 8-bit CPU kullanımı ile eliptik eğriler yönteminin RSA'ya kıyasla performans avantajı getirdiğini ifade etmişlerdir [3].

Xiao Yang, Rayi Venkata Krishna, Sun Bo, Du Xiaojiang, Hu Fei, ve Galloway Michael, kablosuz sensör ağlarında anahtar yönetimine ilişkin 2007 yılında yaptıkları çalışmalarında çeşitli bildirilerde sunulan birçok yöntemi incelemiş, bunların her birinin avantaj ve dezavantajlarını belirlemiş, anahtar yönetimi için yöntem seçiminin güvenlik ihtiyacı gibi gereksinimler ve sahip olunan kaynakları da gözeten bir denge neticesinde ileri sürmüşlerdir [4].

Ciprian Râcuciu, Nicolae Jula, Constantin Balan ve Cosmin Adomnicai, 2008 yılında kendi ürettikleri bir İHA üzerinde; hafif, küçük ve az enerji tüketimine sahip olması nedeniyle Lex Firmasının CV700C ana kartını, şifreleme hızını artırmak maksadıyla Windows XP Embedded işletim sistemini kullanmış, titreşime karşı dayanıklılığını artırmak için İHA üzerindeki hard diski hafıza kartı ile değiştirmiş ve yazılımı DirectShow API2 kullanan C++ ile yapmışlardır. Geliştirdikleri sistem üzerinde şifreleme için Rijndael algoritmasını uygulamış ve İHA üzerindeki kameranın görüntüsünü şifrelemek suretiyle gerçek zamanlı olarak göndermişlerdir. Çalışmada şifreleme modu olarak; Electronic CodeBook (ECB), Cipher Block Chaining (CBC) ve Cipher FeedBack (CFB) kullanılmış ve sonuçları karşılaştırılarak her yöntemin artı ve eksi hususları açıklanmıştır [5].

Chen Xiangqian, Makki Kia, Yen Kang, Pissinou Niki 2009 yılında sensör ağlarında güvenlik üzerine yaptıkları araştırmada özellikle anahtar yönetimi ve ağlarda güvenlik hususlarını incelemiş, tehdit ve zafiyetleri tespit etmiş ve bu hususları yedi başlık altında toplamış, mevcut yöntemlerin her birini bu yedi başlık altında karşılaştırmış ve üzerinde daha çok çalışılması ve önem verilmesi gereken hususları ortaya koymuşlardır [6].

Ren Kui, Yu Shucheng, Wenjing Lou ve Zhang Yanchao ise yine 2009 yılında kablosuz sensör/algılayıcı ağlarında çok kullanıcılı yayın kimlik doğrulaması üzerinde çalışmalarda bulunmuş, özellikle µTESLA ve multilevel µTESLA gibi simetrik anahtar tabanlı yöntemlerin kablosuz sensör ağlarında çok kullanıcılı yayın kimlik doğrulaması konusunda

yetersiz kaldığını ileri sürmüş, ortaya koydukları bu hususları giderebilecek alternatif yöntemler üzerinde çalışmış, sorunu çözmek için asimetrik anahtar tabanlı birkaç şifreleme tekniğinin yeni bir entegrasyonunu önermişlerdir. Bu yöntemle hem işlem hem de iletişim maliyetlerini asgariye indirdiklerini ifade etmiş ve yöntemin etkililiğini ile verimliliğini gösteren, niceliksel bir enerji tüketimi analizi ve güvenlik gücü analizini ayrıntılı olarak gerçekleştirmişlerdir [7].

Munivel E. ve Ajit G.M. 2010 yılında Efficient Public Key Infrastructure Implementation in Wireless Sensor Networks (WSN) konusunda yayımladıkları çalışmada; gizlilik ve yetkilendirmenin hemen hemen her WSN uygulaması için gereken iki önemli güvenlik hizmeti olduğunu, ancak sensör düğümlerinin küçük belleği, zayıf işlemci ve sınırlı pil gücünün, gelişmiş güvenlik tedbirlerini uygulanın önündeki en büyük engeller olduğunu ifade etmişlerdir. Hem bu gereklilik hem de engeller nedeniyle, kaynak kısıtlı sensör düğümlerinde uygulanmak üzere uyarlanmış Açık Anahtar Altyapısının (Public Key Infrastructure-PKI) hafif bir uygulamasını önermişlerdir [8].

Robert Erra, Vincent Guyot, Loica Avanthey, Antoine Gademer ve Laurent Beaudoin, 2012 yılında yayımladıkları ve İHA'da bulunan yazılım ve hassas bilgiyi korumak için, k-ary diye isimlendirdikleri konseptte; Shamir's Secret Sharing Scheme (Shamir'in sır paylaşım tasarımı) ve Neville-Aitken algoritmasının birlikte kullanılarak yüksek seviye güvenlik sağlanabildiği, belirlenen anahtarlarda mod alınmasının, İHA üzerinde bulunan kısıtlı CPU ile şifreleme işlemini kolaylaştırırken, şifrenin kırılmasını zorlaştırdığı ifade edilmiştir [9].

Özgür Koray Şahingöz'ün 2013 yılında İHA'larda ölçeklenebilir kablosuz algılayıcı ağları üzerine yayımlanmış olan konulu çalışmasında İHA'larda veri transferi güvenliğinin sağlanmasına yönelik çok kademeli dinamik anahtar yönetim sistemi geliştirilmesi hedeflenmiş ve çözümün hem yönetilebilir hem de asimetrik tek anahtar yönetim sisteminden daha iyi performansa sahip olduğu belirtilmiştir [10].

Nils Rodday, 2015 yılında yayımladığı çalışmasında İHA'lardaki güvenlik zafiyetlerini incelemiş, bu kapsamda İHA'ların hacklenmesi, GPS aldatma yöntemleri, Wifi-Bluetooth-ZigBee-XBee-KillerBee, radyo dalgaları, "Brute-Force" saldırıları ile veri linkleri üzerinde çalışmış, saldırı ve karşı koyma senaryoları geliştirmiş, güvenlik tedbiri için üç farklı alternatif öneri sunmuş: XBee on-board şifreleme, donanımsal şifreleme ve uygulama

katmanı şifreleme, sonuç olarak; önerilen karşı önlemlerden herhangi birinin uygulanabileceğini ancak bunun İHA üzerinde daha iyi donanım ile daha yüksek üretim maliyeti getirdiğini ifade etmiştir [11].

Wind River Sistem İş Geliştirme, Uzay ve Savunma Müdürü Alex Wilson 2015 yılında yaptığı bir çalışma ile veri linkini, hava aracı, komut ve faydalı yük olarak üç grupta incelemiş, çok kademeli ve uçtan uca güvenli bir sistem kurulması gerektiğini ileri sürmüş, bu maksatla; X.509 tipi bir sertifika, SSL ile korunan veri linki ve kullanıcı yönetim sistemi geliştirilmesi gerektiğini açıklamıştır [12].

Chen Xiao, Lifeng Waog, Mengjiao Zhu ve Wemdong Wang tarafından ise 2016 yılında yapılan çalışmada; öncelikle, video algılama sistemindeki gelişmeler ile kaynak kısıtlamaları incelenmiş, kaynak kısıtlamaları altında bir bilgi-fayda-değer odaklı kaynak etkin şifreleme optimizasyon modeli önerilmiş, bu modele dayanılarak video sıkıştırmasından bağımsız basit bir şifreleme yöntemi geliştirilmiş, bir güvenli video algılama sistemi tasarlanmış ve önerilen şifreleme programı uygulanmıştır [13].

Bu literatür taramasının yanı sıra, kolaylıkla satın alınabilen seri üretim dronlar (rafta) da incelenmiştir. Telemetre (uçuş komutları) için 2,4 GHz, video için 5,8 GHz olmak üzere, genellikle video ve telemetre aktarımı için ayrı kanallar kullanmaktadırlar. Ticari kaygılar nedeniyle güvenlik planda kalmıştır. Kullanıcı, videoyu akıllı telefona veya tablete yüklediği bir program aracılığıyla alabilmektedir. Ancak bu program, herhangi bir kişi tarafından internetten kolaylıkla indirilebilmekte ve sistemlere etki etmek için kullanılabilmektedir. Uçtan uca güvenlik önlemleri bulunmamaktadır; bazıları şifreleme olmadan verileri göndermekte, bazıları da kimlik doğrulama ve yetkilendirme yapmadan görüntü aktarmaya başlamaktadır.

İHA sistemlerinin bu yaygın kullanımı ve önemi göz önünde bulundurulduğunda, karşılaşılabilecek tehlikelerin ve risklerin önceden belirlenmesi ve bu sistemlerin daha da güvenli hale getirilmesi için risk analizinden de faydalanılması gerektiği açıkça görülmektedir. İHA sistemini bir bütün olarak risk analizine tabi tutan çeşitli çalışmalar literatürde bulunmaktadır. Ancak İHA veri linkine ilişkin risk analizine yönelik bir çalışma tespit edilememiş ve ilk defa tarafımızca yapılmıştır. Çalışmamızın son bölümünde İHA veri linkine ilişkin risk analizini esas alacak şekilde, kendi önerdiğimiz güvenli görüntü aktarım

metodu ile literatür taramasında tespit edilen toplam beş yöntemi karşılaştırarak değerlendirmeye tabi tutacak bir yöntem üzerinde durulmuştur. Karşılaştırma ve karar verme için uygun yöntem olarak Çok Kriterli Karar Verme Yöntemi temel alınmış ancak özgün bir yaklaşım olarak kriterlerin belirlenmesi ve alternatiflerin karşılaştırılmasında Risk Analizi metodolojisinden istifade edilmiş, sonuç olarak "Risk Tabanlı Çok Kriterli Karar Verme" yöntemi geliştirilmiştir. Numerik, esnek, objektif, kişiden bağımsız bu yöntem, İHA'lar konusunda Risk Analizi ve Çok Kriterli Karar Verme metodolojisini birlikte kullanmak açısından da yapılan ilk çalışmadır.

Araştırma kapsamında yapılan literatür taramasında risk tabanlı çok kriterli karar verme yöntemlerine yönelik gerçekleştirilen çalışmalar incelenmiştir. Ibrahim M. Khadam ve Jagath J. Kaluarachchi 2003 yılında yayımladıkları çalışmalarında çok kriterli bir karar analiz çerçevesi sağlık riski değerlendirmesi ve ekonomik analizi de kullanarak kirletilmiş yeraltı suyu kaynaklarının yönetimi için entegre bir yaklaşım sunmuşlardır. İzlenen yöntemde, olasılıklı sağlık risk değerlendirmesini kapsamlı, basit ve maliyet temelli çok kriterli karar verme ile birleştirilmiştir. Alternatiflerin sıralanması için kullanılacak üç ayrı yaklaşım belirlenmiştir; yapısal açıklık karar analizi, sezgisel yaklaşım ve bulanık mantık yaklaşımı. Önerilen metodolojiyi göstermek için basit bir sayısal örnek sunulmuştur. Sonuçlar, hem maliyetleri hem de riskleri göz önüne alarak karar vermede bütüncül bir yaklaşım kullanmanın önemini ortaya koyduğu belirtilmiştir [14].

Khan, Sadıq ve Haddara denetleme ve bakım temelli yaptıkları çalışmalarında karar verme modelini risk analizine dayandırmışlardır. Bu çerçevede 2004 yılında yayımladıkları makalede; petrol ve gaz yükleme ve operasyonlarının artan karmaşıklığı, daha yüksek güvenlik seviyeleri sağlamaya yönelik artan toplumsal bilinç doğrultusunda, denetim ve bakım konusunda risk temelli karar vermenin bu tür çözümlerin bulunmasında önem arz ettiği ifade edilmiştir. Bulanık mantığı kullanarak riski (ortaya çıkma ihtimali ve sonucu) çok kriterli karar vermeye dahil eden basit ve yapılandırılmış bir yöntem önermişlerdir. Önerilen metodolojinin etkinliği göstermek açısından, farklı kurumlar tarafından daha önce yapılan bir çalışma kullanılmış ve elde edilen sonuçlar çerçevesinde yöntemlerinin başarılı olduğu ifade edilmiştir [15].

Ying-Ming Wang ve Taha M.S. Elhag, konuyu farklı bir yönden ele almış ve köprülerdeki riskleri belirlemek için bulanık karar verme yönteminden istifade etmişlerdir. Bu çalışma

kapsamında 2007 yılında yayımladıkları makalede; bulanık grup karar verme (fuzzy group decision making approach-FGDM) isminde bir metot önermiş, riskleri olasılık ve sonucun bir birleşimi olarak metoda dahil etmiş, elde edilen sonuçları da güvenlik, fonksiyon, sürdürülebilirlik ve çevre açısından değerlendirmişlerdir. Çalışma neticesinde bulanık grup karar verme yönteminin köprü risklerinin modellenmesi için esnek, pratik ve etkili bir yol olduğunu ileri sürmüşlerdir [16].

2009 yılındaki çalışmalarında, Robin Dillon, Robert Liebe ve Thomas Bestafka; antiterör tedbirlerinin belirlenmesi ve önceliklendirilmesi için risk esasına dayalı karar desteği (risk-based decision aid-ARDA) adını verdikleri bir yöntem önermişlerdir. ARDA modelinin, ABD Deniz Kuvvetleri'nin tesis, araç, silah ve teçhizatını maliyet etkin ve riski en aza indirecek uygun tedbirlerin alınıp alınmadığını kontrol etmek için geliştirildiği belirtilmiştir. Çalışmada, 160 tesis tipine yapılabilecek 15 saldırı tipi incelenerek 22 alternatif hareket tarzı karşılaştırılmıştır [17].

Ravi Ravindrana, Ufuk Bilsela, Vijay Wadhwab ve Tao Yang 2009 yılında yaptıkları çalışmada; tedarikçi riskini içeren çok sektörlü tedarikçi seçme modeli üzerinde durmuş, iki farklı risk modeli önermişlerdir; "riske maruz değer" ve "hedefi kaçırma". Risk odaklı tedarikçi seçimi problemini çok kriterli bir optimizasyon problemi olarak modellemiş, tedarikçi seçim süreçlerini optimize etmek için risk sınıflandırması ve niceleme yöntemleri ile kesikli ve sürekli çok kriterli karar verme tekniklerinin uygulamışlardır [18].

M.D. Catrinu ve D.E. Nordgard, belirsizlik altında elektrik dağıtım sistemi varlık yönetimi konusunda risk analizi çok kriterli karar vermeyi birleştirerek bir model geliştirmiş ve bu konuda 2011 yılında bir makale yayımlamışlardır. Çalışmanın odak noktası, elektrik dağıtım şebekesinin fiziksel varlıklarını nasıl ele alacağına karar verirken, farklı şirket hedeflerini ve risk analizlerini yapısal bir karar çerçevesine nasıl dahil edeceği üzerine kurulmuştur. Ayrıca, belirsizlik altında uzman bilgisi, basitleştirilmiş risk analizleri ve çok kriterli karar analizi kullanılarak, bakım ve yeniden yatırım stratejileri için karar desteğine açıklayıcı bir örnek de sunulmuştur [19].

Athanasios C. Karmperis, Anastasios Sotirchos, Konstantinos Aravossis ve Ilias Tatsiopoulos 2011 yılında yayımladıkları çalışmalarında, kantitatif bir risk analizi ile bir atık yönetim projesinin alternatiflerinin değerlendirilmesi incelemişlerdir. Bu çalışmada, bir atık

yönetim projesinin optimum alternatifini seçmek için karar alıcılar tarafından kullanılabilen, riske dayalı çok kriterli değerlendirme (risk-based multi-criteria assessment-RBMCA) adında yeni bir yaklaşım getirdiklerini, yöntemde, kriterlerin ağırlık değerleri ile karar vericilerin risk tercihleri arasındaki korelasyonun analiz edilerek bir karara ulaşıldığını ileri sürmüşlerdir [20].

Yao-Chen Kuo ve Shih-Tong Lu ise 2012 yayımladıkları makalede, güvenilir bir risk değerlendirme modeline ihtiyaç duyan metropolitanlarda inşaat projelerinde kullanılmak üzere sistematik olarak risk değerlendirmek için bulanık çok kriterli karar verme (fuzzy multiple criteria decision making-FMCDM) yaklaşımını önermişlerdir. Belirledikleri yirmi risk faktörünün proje performansı üzerindeki nispi etkisini ölçmek ve araştırmak için tutarlı bulanık tercih ilişkileri (consistent fuzzy preference relations-CFPR), birden çok risk faktörünün ortaya çıkış olasılığını analiz etmek için de bulanık çoklu özellikler direkt derecelendirme (fuzzy multiple attributes direct rating-FMADR) yaklaşımını kullanmışlardır. FMCDM'nin uygulanmasının, önerilen risk değerlendirme yaklaşımını geleneksel istatistiksel yaklaşımdan daha güvenilir ve pratik hale getirdiğini, önerilen yaklaşımın, genel proje riskini etkili bir şekilde değerlendirmek için kullanılabileceğini ve bir metropol inşaat projesinin önemli risklerini etkin bir şekilde tanımlamak için yararlanılabileceğini ifade etmişlerdir [21].

Literatür taramasında genel olarak karşılaşılan yöntemler, tam bir risk analizini veya değerlendirmesini içermeyip çoğunlukla risklerin bir olasılık olarak karar modeline dahil edilmesine ve alternatiflerin bu olasılıklar da göz önünde bulundurularak karşılaştırılmasına dayanırken bizim önerdiğimiz yöntemde farklı olarak, risk yönetiminin ilk adımı olan risk değerlendirmesi ve analizi tamamıyla icra edilmiş, bu amaçla ön tehlike listesi ve ön tehlike analizi metotları ile güvenlik blok diyagramı kullanılmış, sonucunda elde edilen tehlike listesi ve şiddet ile olasılığın çarpımı olarak ifade edilen risk çok kriterli karar verme yönteminde girdi olarak kullanılmıştır. Risk analizinden alınan tehlike listesi alternatifleri, risk ise alternatiflerin ağırlıklarını oluşturmuş, böylece risk analizi doğrudan kararı etkilemiştir.

Karar verme sürecinde, basitliği ve amaca uygunluğu nedeni ile Ağırlıklı Toplam Yöntemi çok kriterli karar verme modeli olarak belirlenmiş, hem tecrübe ve bilgiden hem de sayısal olgu ve verilerden istifade edilmek esas alındığından kalitatif ve kantitatif karışımı hibrit bir

yaklaşım tercih edilmiştir. Karar matrisi oluşturulurken sayısal ağırlık ve oranlardan istifade edilmiş ancak bu ağırlık ve oranlar uzman grubun bilgi ve tecrübelerine dayalı olarak tespit edilmiştir. Karara niceliksel olarak ulaşabilmek adına alternatiflerin her bir kriteri ne oranda karşıladığını belirlemek için "Kriter karşılama oranı-KKO" kullanılmıştır. Her bir kriter için ağırlık ve KKO çarpımı da "Değer" olarak isimlendirilmiştir.

Yukardaki bilgiler ışığında hazırladığımız tez 7 bölümden oluşmaktadır. İkinci bölümde İHA'nın tanımı ve tarihçesi ile birlikte kullanım alanları, tasnifi ve unsurlarından bahsedilmiş, örnek bir 3 boyutlu İHA modeli oluşturularak analiz sonuçları verilmiştir. Üçüncü bölümde İHA'ların haberleşmesi, frekans planlama ve tahsis kriterleri açıklanmış, genel olarak RF haberleşme ve sinyal istikameti bulma yöntemlerine ayrılmıştır. Dördüncü bölümde İHA'lara karşı yapılabilecek saldırı türleri, örnek olaylar ile alınması gereken tedbirlere değinilmiştir. Beşinci bölümde mevcut kripto yöntemleri incelenmiştir. Altıncı bölümde İHA'larda kullanılmakta olan güvenli veri aktarım ve kriptolama yöntemleri ile örnek ele geçirme olayları araştırılarak geliştirilen güvenli veri aktarım yöntemi detaylı olarak izah edilmiş, ardından geliştirilen güvenli görüntü aktarım yönteminin İHA uçuş güvenliğine katkısı ve önerilen yöntemin literatür taramasında tespit edilen diğer yöntemlerle risk tabanlı çok kriterli karar verme metodu ile karşılaştırma sonuçları verilmiştir. Son bölümde ise elde edilen sonuçlar değerlendirilerek önerilen metodun avantaj ve dezavantajları ile bundan sonra yapılması gereken çalışmalardan bahsedilmiştir.

2. İNSANSIZ HAVA ARACI

İnsansız teknolojilerin kullanımının yaygınlaşmasının altında gelişen teknolojinin sağladığı imkânla birlikte bazı maliyetli ya da sorunlu kalemleri aşabilmenin getirisi bulunmaktadır. İnsansız uçakların otonom ya da bir yer istasyonu aracılığıyla kontrol edilebiliyor olması insanlı uçakların idamesi için gerekli yaşamsal sistemler ve kokpit için gerekli yer ve mürettebatın getirdiği ağırlık yükü gibi maliyet kalemleri, insanlı uçakların manevra ve operasyon kabiliyetinin insan kabiliyetleriyle sınırlanması (yorgunluk / çalışma saati, G kuvveti vb.) gibi operasyonel kabiliyetle ilgili kalemler, düşman tarafından fark edilme ya da vurulabilme olasılığının düşük olması üstünlük kalemleri İHA'ları daha tercih edilir kılmaktadır.

Daha da önemlisi, İHA'ların zayiat maliyetidir. Tüm dünya ordularında yetiştirilmesi en maliyetli personel gruplarından birisi pilotlardır. Bir pilotun yetişmesi çok büyük maliyetlere karşılık gelir. Bu sebeple hava aracıyla zayiatıyla birlikte yetişmiş personelin de zayi olması ordular için hem maddi hem de kabiliyet olarak büyük kayıptır. İnsansız Hava Araçları, zayiat maliyetinin düşük olması açısından da orduları cezbetmektedir. İHA'lar tarihte birçok kez düşman hava savunma unsurlarının oyalanmasında, asıl taarruz unsurlarının ateş hattını geçebilmesi için yem olarak kullanılmasında çok büyük rol oynamışlardır [22].

Dünya çapında altmışın üzerinde ülke İHAS üretmesine rağmen halen bu uçaklara yapılan yatırımda yüzde 76 pay sahibi olan ABD'dedir. ABD'de bir yılda eğitilen İHA pilotu sayısı 2012 yılından itibaren bir yılda eğitilen jet pilotlarının sayısını geçmiştir.

2030 yılında 30 bin İHA'nın semalarda olacağı öngörülmekte; küresel pazar payının 2020 yılına kadar, askeri maksatlı 11,6 milyar dolar, ticari amaçlı 6,4 milyar dolar ve hobi amaçlı 4,4 milyar dolar olmak üzere toplam 22,4 milyar dolara ulaşacağı tahmin edilmektedir.

ABD'deki Hollaman Hava Üssü gibi askeri İHA eğitim alanlarının yanı sıra 150 kadar Amerikan üniversitesi de bu alanda sivil personel yetiştirmek için eğitim programları açmış durumdadır. Hatta bunların içinden Florida'da bulunan Embry-Riddle Aeronautical Üniversitesi ve North Dakota Üniversitesi lisans düzeyinde dört yıllık program başlatmıştır. ABD'de bu alana yeni bir istihdam sahası gibi bakılmaya başlanmasının ve bir trende

dönüşmesinin arkasında yakın bir gelecekte askeri operasyonlar haricinde bu teknolojinin sivil operasyonlarda da etkin olarak kullanılacağı inancı ve böylece oluşacak büyük pazardan şimdiden pay alma düşüncesi yatmaktadır.

İHA'ların bugün kullanıldığı gibi askeri amaçlar dışında atmosfer gözlemleme, hava tahmini ya da bilimsel araştırma, boru hatları takibi, yol kontrolü, arama ve kurtarma çalışmaları, hava fotoğrafçılığı, petrol, gaz ve mineral araştırmaları ile kargo/kurye hizmetleri gibi sivil sahalarda kullanılmaya başlanması ile birlikte büyük bir ticari potansiyelin ortaya çıkabileceği öngörülmektedir [23].

2.1. İnsansız Hava Araçlarının Sivil Kullanım Alanları

Sivil kullanım alanları; güvenlik ve kontrol, afet etkilerinin yönetimi tarımsal faaliyetler ve diğer adı altında dört ana bölümde sınıflandırılmaktadır.

- Güvenlik ve kontrol: Polisiye amaçlı yukarıdan gözetleme, hava durumu raporlama, havadan tarama, inşaat sektörü, şehir planlamaları, kaçak yapılanmaların tespiti, su ve ulaşım yollarının kontrolü, gaz ve petrol boru hatlarının güvenliği, balıkçılık sektörü.
- Afet etkilerinin yönetimi: Kurtarma ve afet sonrası temizlik işleri, afet hasar tahminleri.
- Tarımsal faaliyetler: Zirai ilaçlamalar, tarım alanları, erozyon ve orman yangınlarının kontrolü gibi konular sivil kullanım olarak sayılabilmektedir. Bu gruplamalar daha da çoğaltılabilir [24].
- Diğer: Hobi maksatlı, fotoğrafçılık, kurye, kargo vb.

2.2. İnsansız Hava Araçlarının Askeri Kullanım Alanları

İHA sistemlerinin görevleri ile ilgili başarılı bir tasnif çalışması Savunma Sanayi Müsteşarlığı (SSM) tarafından hazırlanan 2011-2030 İHA Sistemleri Yol Haritası dokümanında yapılmıştır. Temel olarak Keşif/ Gözetleme Desteği, Taarruz, Elektronik Harp, Hedef Benzetimi ve Özel/Spesifik Görevler olmak üzere 5 alanda yapılan bu tasnif dahilinde İHA'ların askeri kullanım alanları Çizelge 2.1'de sunulmuştur.

Çizelge 2.1. İHA'ların askeri kullanım alanları [25]

Keşif / Gözetleme Desteği	Taktik Saha Keşif / Gözetleme Stratejik Keşif / Gözetleme
Taarruz	İç Güvenlik Yakın Hava Desteği Hava Savunma Sistemlerinin İmhası Hava Sahası Savunma
Elektronik Harp	Sinyal İstihbaratı Radar Elektronik Harp Muhabere Elektronik Harp Önleyici Elektronik Harp
Hedef Benzetimi	Hedef Uçak Sahte Uçak
Özel / Spesifik Görevler	Haberleşme Desteği Mayın / Patlayıcı Tespit Kimyasal, Biyolojik, Radyoaktif, Nükleer Tespit Deniz Karakol / Denizaltı Savunma Harbi Arama-Kurtarma/Lojistik

2.3. İnsansız Hava Araçlarının Tasnifi

Askeri amaçlı İHA'larla ilgili farklı sınıflamalar mevcuttur. Bu sınıflamalar kısaca şu şekilde özetlenebilir:

- Büyüklük, irtifa, uçuş süresi ve faydalı yük kapasitesine göre: Micro-Mini-Küçük-Taktik-Operatif-Stratejik,
- Faydalı yük türüne göre: Silahlı İHA'lar - Silahsız İHA'lar,
- Yakıt türüne göre: İçten yanmalı motorlu - Elektrik motorlu İHA'lar,
- Uçuş yöntemine göre: Sabit Kanatlı - Döner Kanatlı,
- Komuta biçimine göre: Otomatik pilotlu - Uzaktan komutalı,
- Kullanım amacına göre: Sahte/Hedef - Keşif Gözetleme - Atak/Saldırı - Lojistik destek,
- Kalkış ve iniş yöntemine göre: Rampadan kalkan/fırlatılan - Pistten kalkan - Uçaktan bırakılan - elle fırlatılan - gövde üzerine iniş yapan - paraşütle iniş yapan.

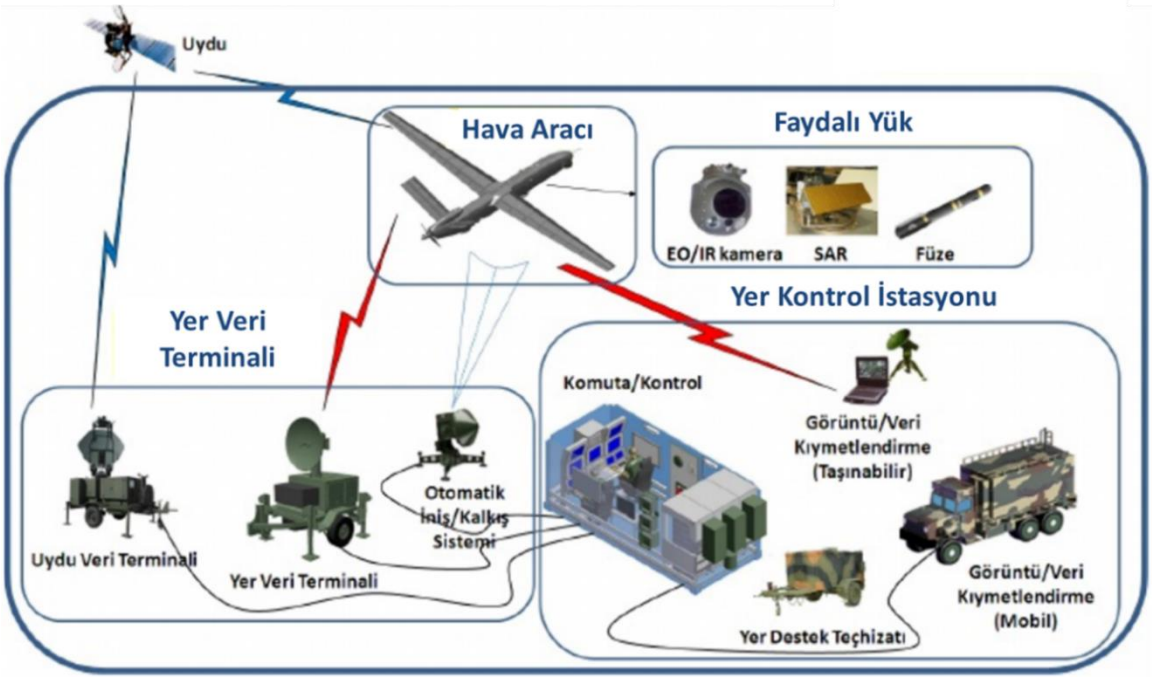
İHA'lar büyüklüklerine ve diğer temel özelliklerine göre yukardaki tasnife de uygun olarak üç sınıfta toplanmaktadır. Söz konusu İHA tasnif metoduna göre temel ayırt edici özellikler Çizelge 2.2'de verilmiştir.

Çizelge 2.2. İHA tasnif metoduna göre temel ayırt edici özellikler [26]

Sınıf	Kategori	Operasyon İrtifası (feet-AGL)	Menzil Yarıçapı (km)	Havada Kalma Süresi (saat)
Sınıf 1 (<150 kg)	Mikro <2 kg	200	5	1
	Mini 2-20 kg	3.000	25	<2
	Küçük >20 kg	5.000	50	3 - 6
Sınıf 2 (150-600kg)	Taktik	10.000	200	6 - 10
Sınıf 3 (>600kg)	Operatif (MALE)	45.000	Sınırsız	24 - 48
	Stratejik (HALE)	65.000	Sınırsız	24 - 48
	Taarruz - Atak	65.000	Sınırsız	>48

2.4. İnsansız Hava Aracı Sistemi Unsurları

İHA sistemi dört temel unsurdan oluşmaktadır: İHA, Yer Veri Terminali (YVT), Yer Kontrol İstasyonu (YKİ). Ayrıca, jeneratör, ekipman ve yakalama kancası gibi unsurları içeren yer destek teçhizatı da mevcuttur. İHAS unsurları Şekil 2.1'de sunulmuştur.

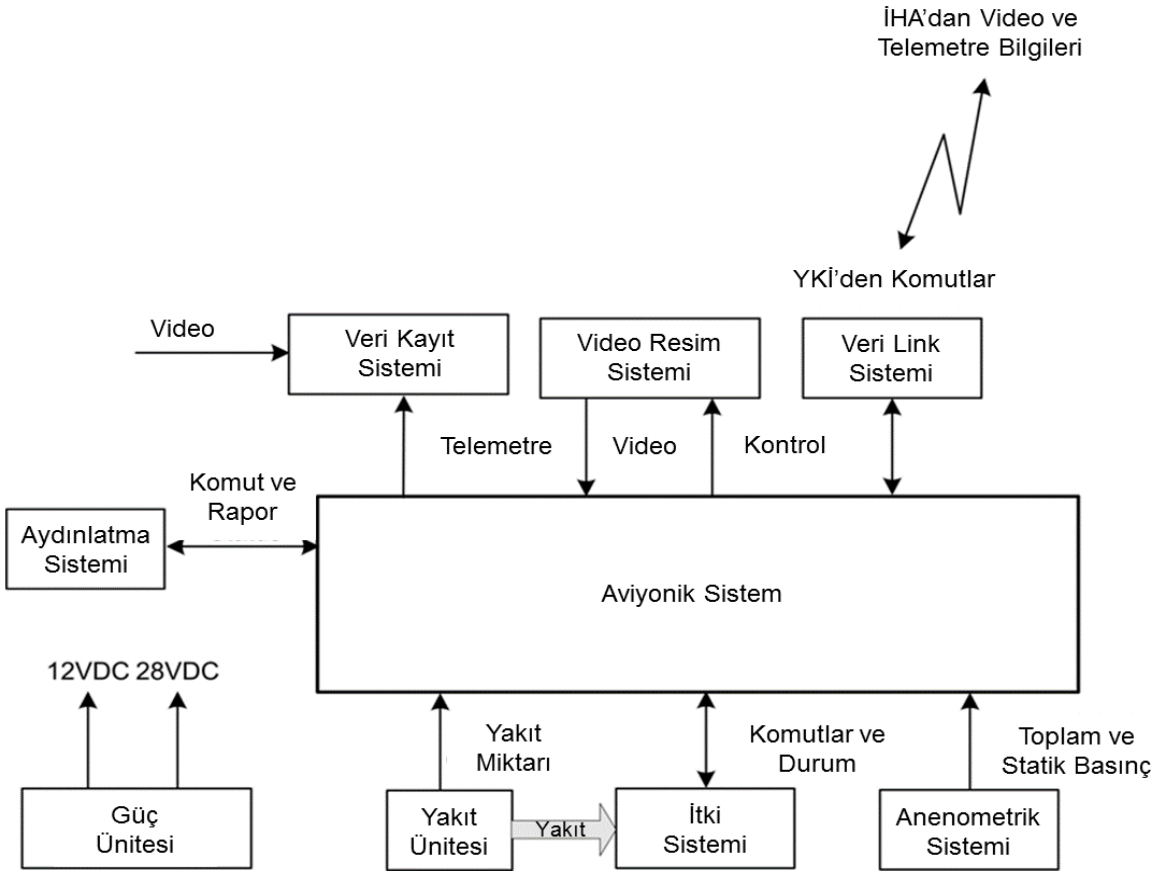


Şekil 2.1. İHAS unsurları [25]

2.4.1. Hava aracı

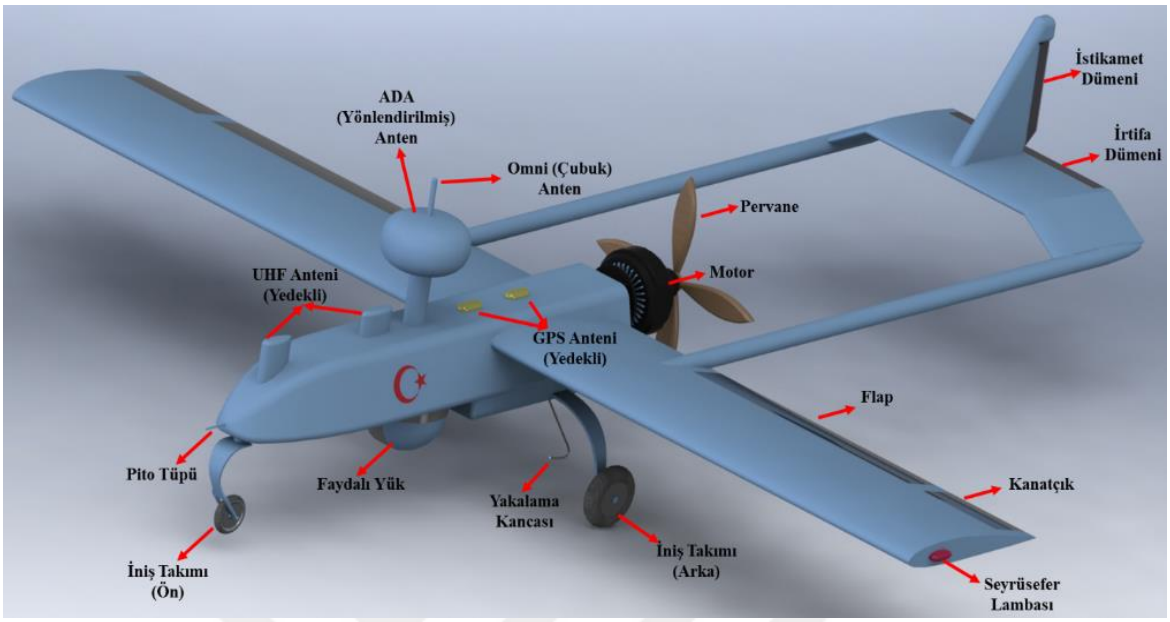
Şekil 2.2'de bulunan, bir İHA'nın alt sistemleri genel olarak aşağıda sunulmuştur.

- Aviyonik sistem (İngilizce Avionics: Aviation Electronics): havacılıkta uçaklar, yapay uydular ve uzay araçlarının elektronik sistemlerini için kullanılan terimdir. Aviyonik sistemleri arasında haberleşme, seyrüsefer, birden fazla sistemin görüntü ve yönetimi ve bireysel işlevleri gerçekleştirmek için uçaklara takılan yüzlerce sistem sayılabilir.
- İtki sistemi: Motor, pervane ve varsa motor bilgisayarından oluşmaktadır.
- Yakıt sistemi: Yakıtın depolanması, miktarının, ısısının ve basıncını ölçülmesi ile motora aktarılmasını sağlayan bileşenlerden oluşmaktadır.
- Elektrik sistemi: Hava aracındaki elektriğin motor veya alternatörden itibaren alt bileşenlere ulaşmasını sağlayan unsurlardan müteşekkildir.
- Veri linki (haberleşme) sistemi: Asıl konu olduğundan aşağıda incelenecektir.



Şekil 2.2. İHA'nın alt sistemleri

Bir hava aracının üzerinde genel olarak Şekil 2.3'deki unsurlar bulunmaktadır.



Şekil 2.3. Hava aracının üzerinde bulunan unsurlar

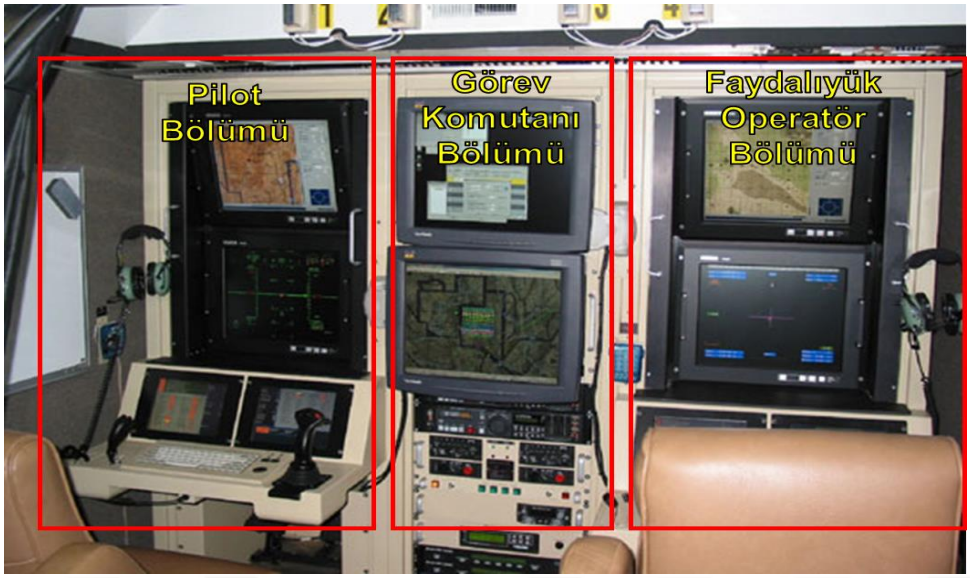
2.4.2. Yer kontrol istasyonu

İHA'nın ve faydalı yükün gerçek zamanlı kontrollerini sağlayan, raporlarını alan sabit/mobil ünitedir. Örnek yer kontrol istasyonları (YKİ) Resim 2.1'de görülmektedir.

a) b)

Resim 2.1. Örnek YKİ'ler a) Araca monte [27] b) Konteynır [28]

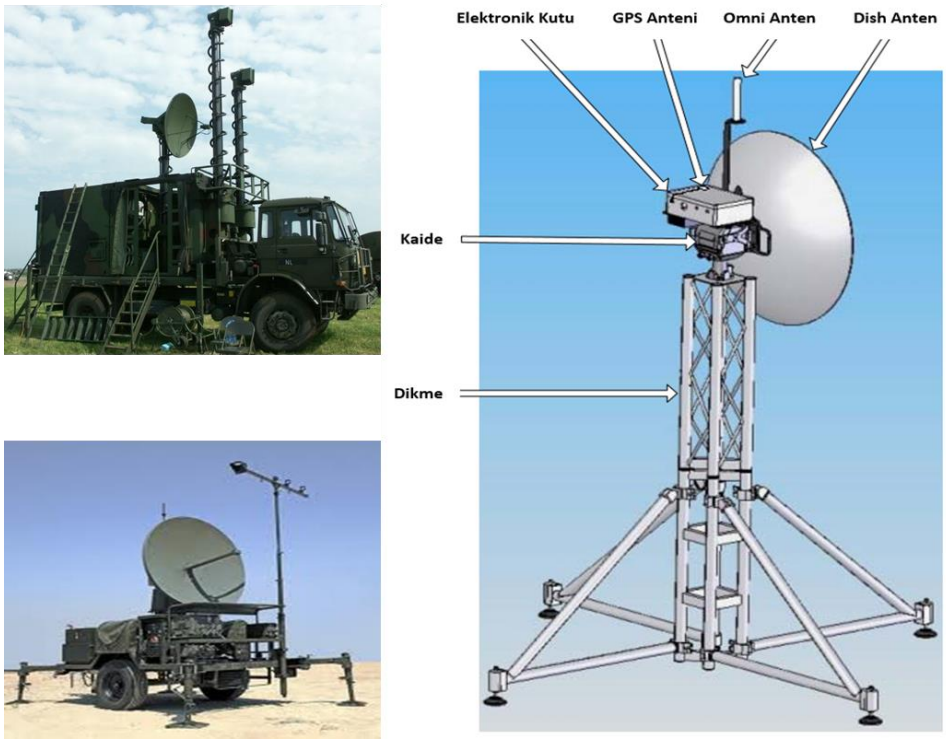
YKİ iç kısmında Resim 2.2'de görüldüğü gibi pilot ve faydalı yük operatörünün sistemleri kontrol ettikleri bölümler bulunmaktadır.



Resim 2.2. YKİ iç kısmı [29]

2.4.3. Yer veri terminali

İHA ile YKİ arasındaki kablosuz veri iletişimini (Q, C, S, UHF bantları vb. üzerinden) sağlayan mobil/sabit entegre anten ve elektronik sistem ünitesidir. Örnek yer veri terminalleri (YVT) ve ana parçaları Resim 2.3'de görülmektedir.



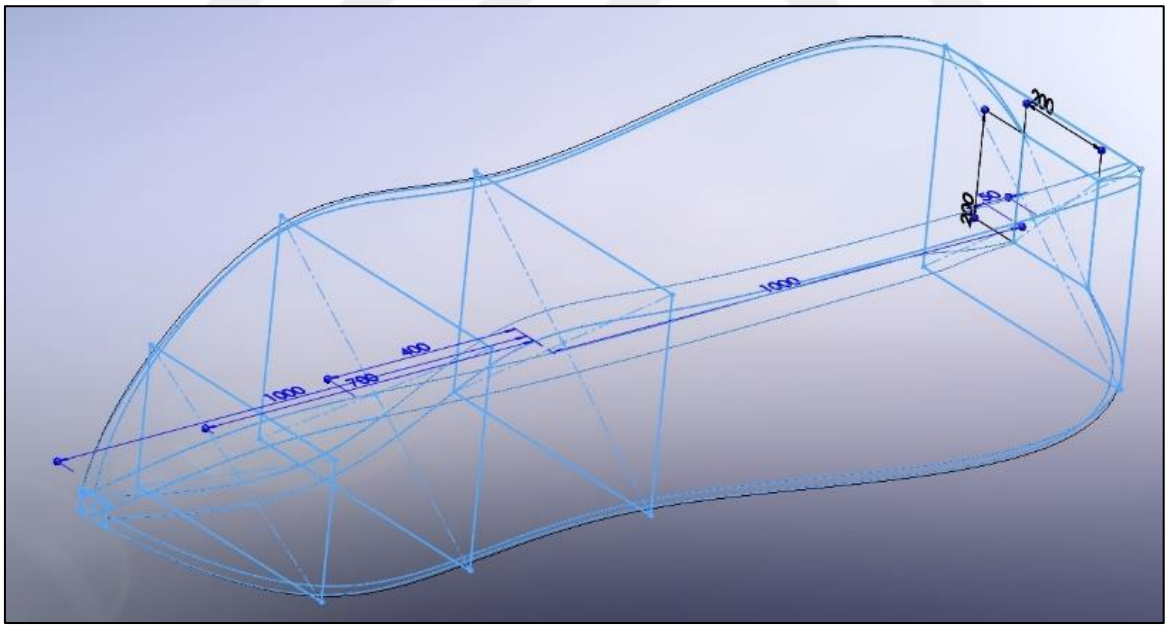
Resim 2.3. Örnek YVT ve ana parçaları [30, 31]

Yukarıda verilen bilgiler ışığında çalışmada da kullanılmak üzere örnek bir üç boyutlu İHA modeli oluşturulmuş ve yapısal analizi gerçekleştirilmiştir.

2.5. Üç Boyutlu İnsansız Hava Aracı Modelinin Oluşturulması

Çalışmanın maksadı optimum İHA tasarımını bulmak değil, modelleme ve simülasyon açısından bir modelin adım adım nasıl oluşturulduğunu ve bahse konu modelden istifade ile belirlenen konuda analiz için nasıl kullanıldığını göstermektir. Bu nedenle mevcut olan herhangi bir modelle kıyaslama ya da tasarımın artı yönlerini ortaya koyma yoluna gidilmemiştir. Aynı nedenlerden dolayı tasarım ve analiz için kullanılan program ve araçlara da değinilmesine gerek görülmemiştir.

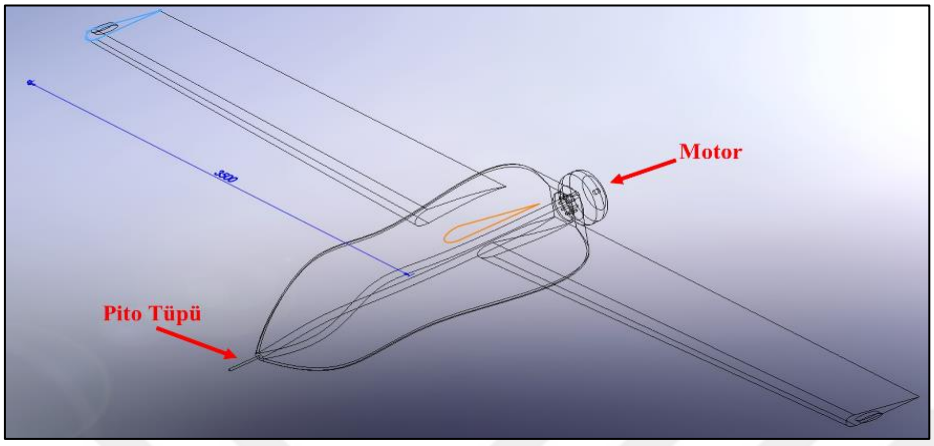
Üç boyutlu İHA tasarımına öncelikle gövdeden başlanmıştır. Şekil 2.4'de sunulan gövde tasarımında görüldüğü gibi 6 farklı ölçüde dikdörtgenin birleştirilmesi neticesinde uzunluğu 2 m., genişliği 0,6 m., yüksekliği 0,45 m. olan gövde tasarımı elde edilmiştir.



Şekil 2.4. Gövde tasarımı

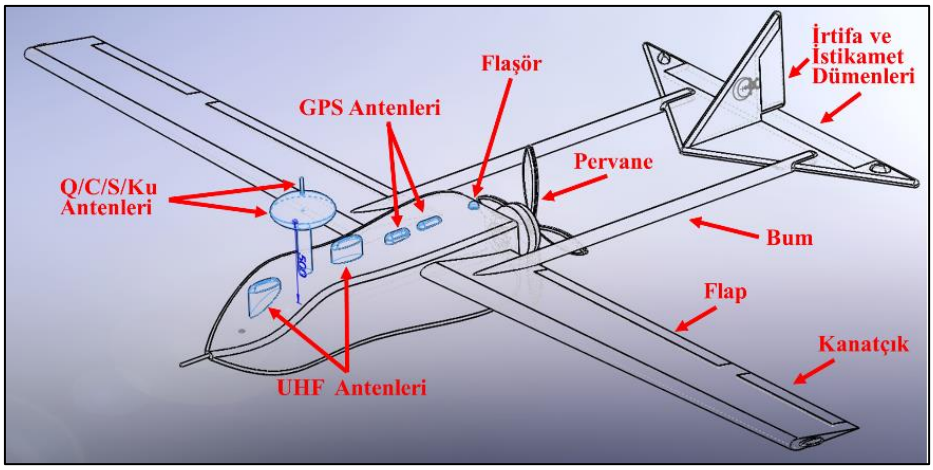
Modele bir motor ve pito tüpü (toplam başın ölçümü için kullanılan boru şeklindeki aparat)'nün ardından ortadan dışa uzunluğu 3,5 m. olmak üzere uçtan uca toplam 7 m.lik kanat ilave edilmiştir. Pito tüpü, motor ve kanatlar Şekil 2.5'de sunulmuştur. Kanatlarda,

irtifa alama/verme maksadıyla kullanılan iki adet flap ile havada dönüşleri sağlayan iki adet kanatçık oluşturulmuştur.



Şekil 2.5. Pito tüpü, motor ve kanatlar

Müteakip safhada motor miline entegre temsili bir ahşap pervane oluşturulmuştur. Kanatlara bağlanan iki adet bum ile kuyruk bölümünde bulunan irtifa ve istikamet dümenleri gövdeye bağlanmıştır. Bumlar ayrıca kuyruktaki aydınlatma ve elektronik sistemlere güç ve veri sağlayan kabloların içerisinden geçirilmesi amacına da hizmet etmektedir. Gövde üstünde; Q/C/S/Ku bantları için iki, UHF bandı için iki olmak üzere veri linki sistemine dâhil olan toplam dört adet anten yerleştirilmiştir. Bunlara ilave olarak yer belirleme sistemi olan GPS için yine biri yedek olmak üzere iki adet anten ile flaşör de gövde üzerinde konumlandırılmıştır. Bahsedilen bu unsurların bulunduğu kanat/kuyruk bölümü ve antenler Şekil 2.6'da sunulmuştur.



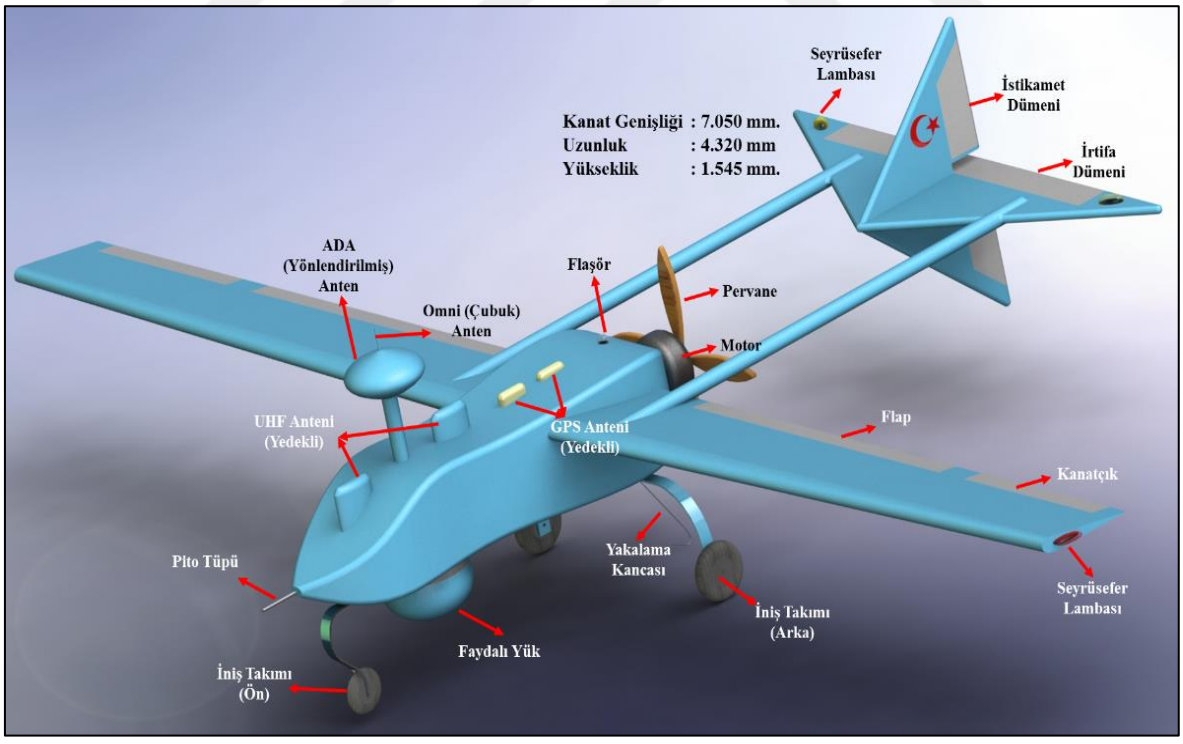
Şekil 2.6. Kanat/Kuyruk bölümü ve antenler

Son safhada dönebilen bir ön teker, iki sabit arka teker ve yakalama kancasından oluşan iniş takımı ile bir faydalı yük olan kamera modele ilave edilmiştir. İniş takımları katlanamaz şekilde dizayn edilmiş ve fren tertibatı yerine uçağı durdurmak üzere yakalama kancası tercih edilmiştir.

İHA modelinin bir bütün olarak tasarlanmasının ardından iniş takımlarının ilgili bölümleri için metal ve lastik, seyr-ü sefer ışıkları için şeffaf plastik ve gövdenin tamamı için ahşap malzeme seçilmiştir.

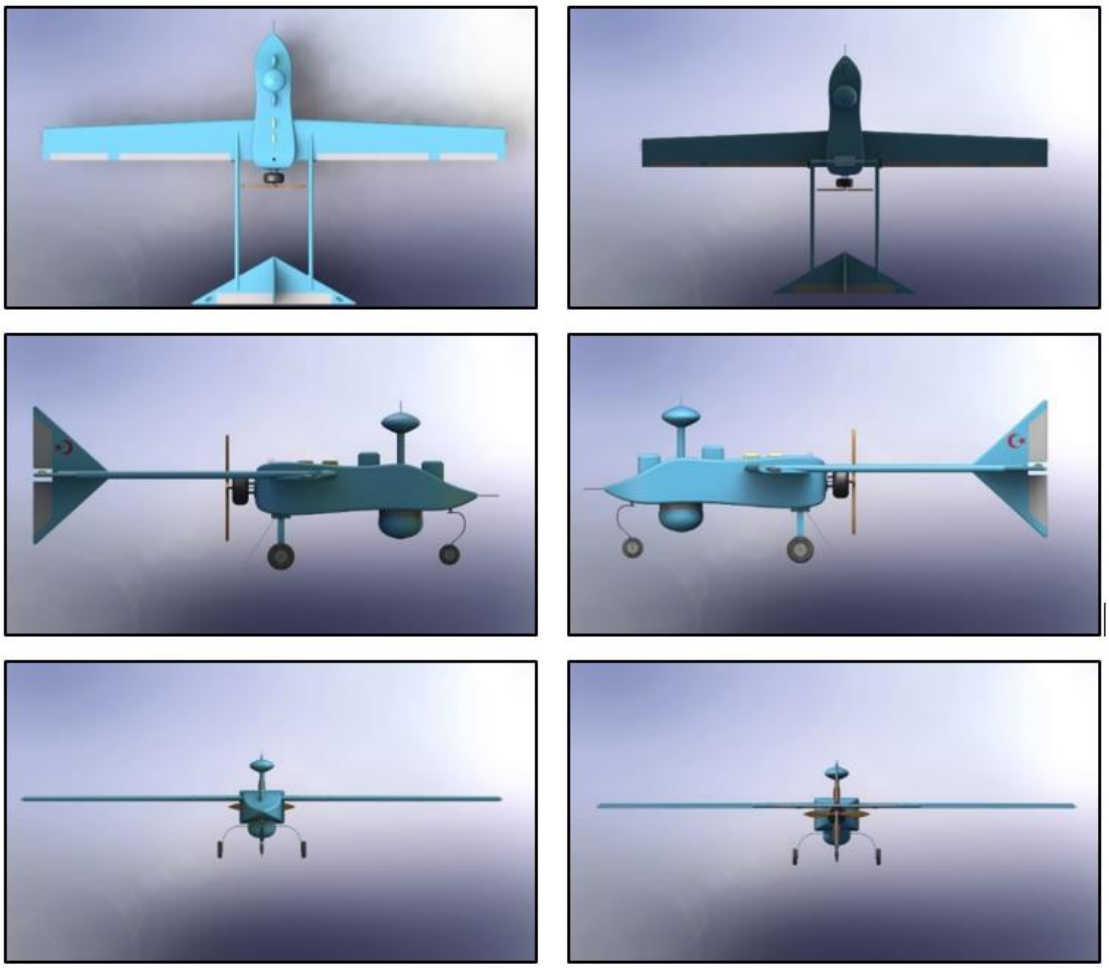
Modelin tasarlanması esnasında, var olan herhangi bir İHA'nın ölçülerinden faydalanılmamış, değerler tamamen tecrübi olarak belirlenmiştir. Özellikle kuyruk bölümünün "+" şeklindeki görünümü, tek parçalı irtifa dümeni ve iki parçalı istikamet dümeni ile yenilikçi bir tasarım tercih edilmiştir.

Tamamlanmış 3B İHA modelinin boyutları ve ana parçaları Şekil 2.7'de görülmektedir.



Şekil 2.7. Tamamlanmış 3B İHA modelinin boyutları ve ana parçaları

3B İHA modelinin üstten, alttan, yanlardan, önden ve arkadan görünümü Şekil 2.8'de sunulmuştur.



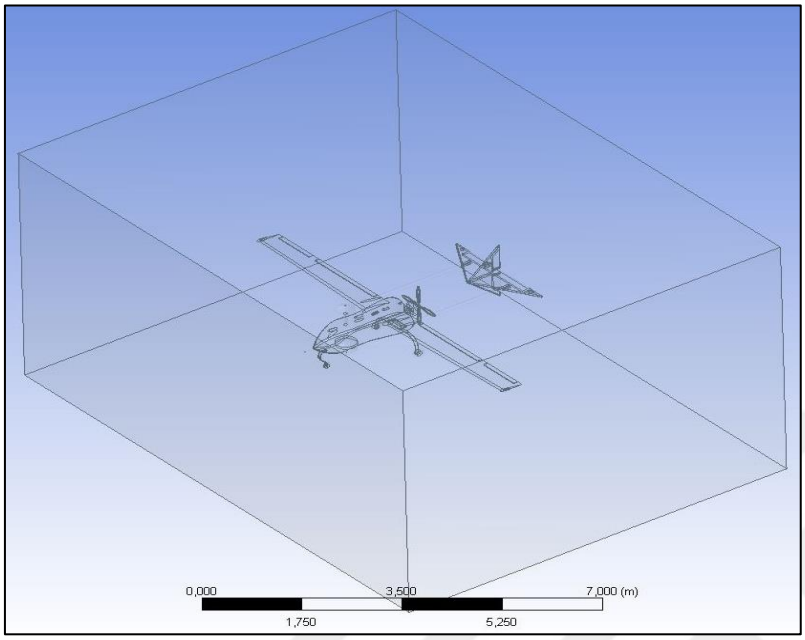
Şekil 2.8. 3B İHA modelinin üstten, alttan, yanlardan, önden ve arkadan görünümü

2.6. İnsansız Hava Aracı Modelinin Sonlu Elemanlar Metoduyla Akış Analizi

Sonlu elemanlar metoduyla akış analizini yapabilmek için öncelikle tasarladığımız 3B İHA modeli sisteme eklenir ve gerçek şartlara uygun hava akışı simüle edilebilmesi maksadıyla bir hava kütlesi tasarlanır. Belirlenen hava kütlesinin İHA'yı içine alacak boyutlarda tasarlanması önem arz etmektedir [32].

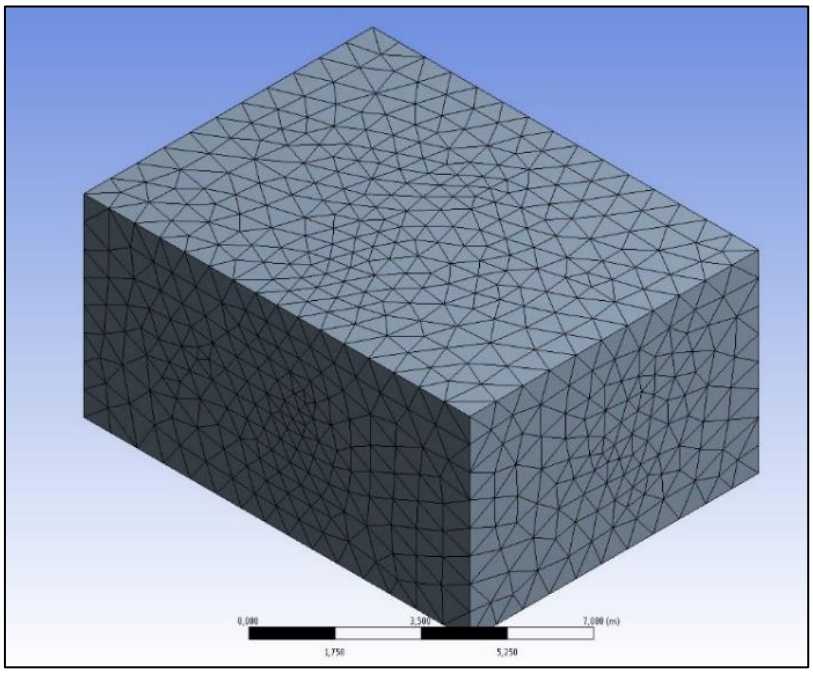
Kütlenin hava giriş yüzeyi, hava çıkış yüzeyi, diğer yüzeyler ve hava içerisindeki uçağın yüzeyleri belirlenerek hava akışının nereden ve nasıl etki edeceği tanımlanmıştır. Şekil 2.9'da hava aracı ve hava kütlesinde oluşturduğu alan gösterilmektedir. Hava kütlesinin dış yüzeyi ile uçak yüzeyi arasındaki tolerans alan oldukça fazla bırakılarak uçağın etrafında oluşacak türbülans ve vorteks etkilerinin de analiz edilmesine imkan sağlanmıştır. Aradaki

hava alanının fazla olmasının sonuca olumsuz bir etkisi bulunmayıp sadece işlem süresini artırmakta, bununla beraber grafikteki geçiş bölgeleri daha net görülebilmektedir.



Şekil 2.9. Hava aracı ve hava kütlesinde oluşturduğu alan

Sonlu elemanlar metoduyla analiz yapılabilmesi için model hacmi çıkartılarak ilk mesh işlemi sonucu oluşturulan hava kütlesi Şekil 2.10'daki gibi bir ağ yapısına dönüştürülmüştür.



Şekil 2.10. İlk mesh işlemi sonucu oluşturulan hava kütlesi

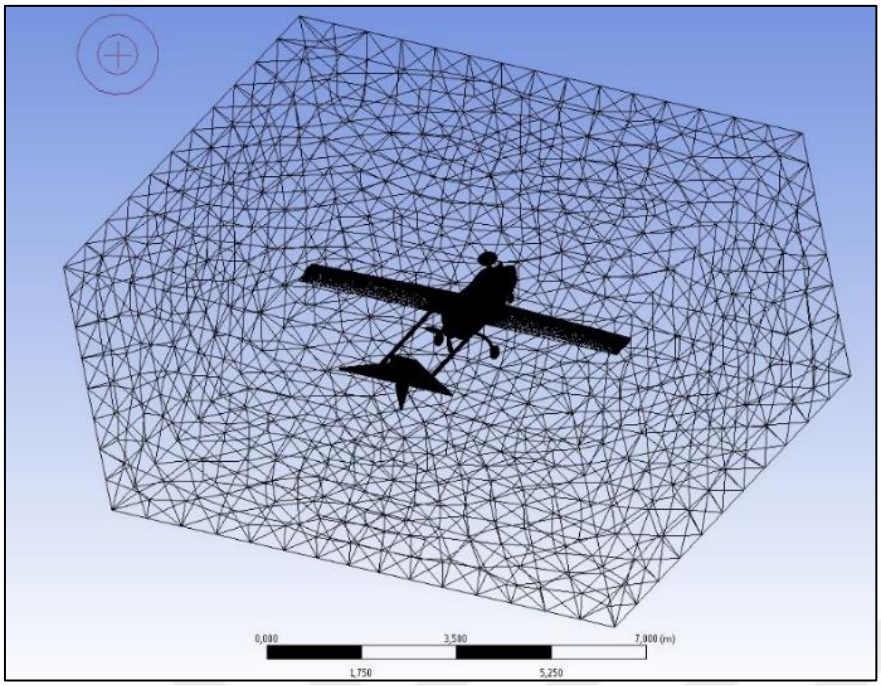
Analiz hassasiyetinin yüksek tutulabilmesi ağ yapısına ilişkin parametrelerin (merkez nokta, sıkışıklık, ortagonallik vb.) doğru belirlenmesi ile mümkün olabilmektedir. Bu nedenle analiz için yeterli kalite sağlanana kadar yeniden parametrelerin yeniden düzenlenmesi gerekmektedir. Bu çalışmada kullanılan parametreler Çizelge 2.3'de sunulmuştur.

Çizelge 2.3. Kullanılan parametreler

Parametreler	Başlangıç Değerleri	Son Değerler
Advance size Function	Curvature	Curvature
Relevance Centre	Coarse	Fine
Initial Size Seed	Active assembly	Full assembly
Smoothing	Medium	High
Transition	Fast	Slow
Span Angle Centre	Coarse	Fine
Curvature Normal Angle	Default (18)	Default (18)
Min Size	Default(7,4337e-0003m)	6,0e-003m
Max face Size	Default (0,743370m)	Default (0,743370m)
Max Size	Default (1,4867m)	Default (1,4867m)
Growth Rate	Default (1.20)	Default (1.20)
Minimum Edge Length	4,5205e-007m	4,5205e-007m

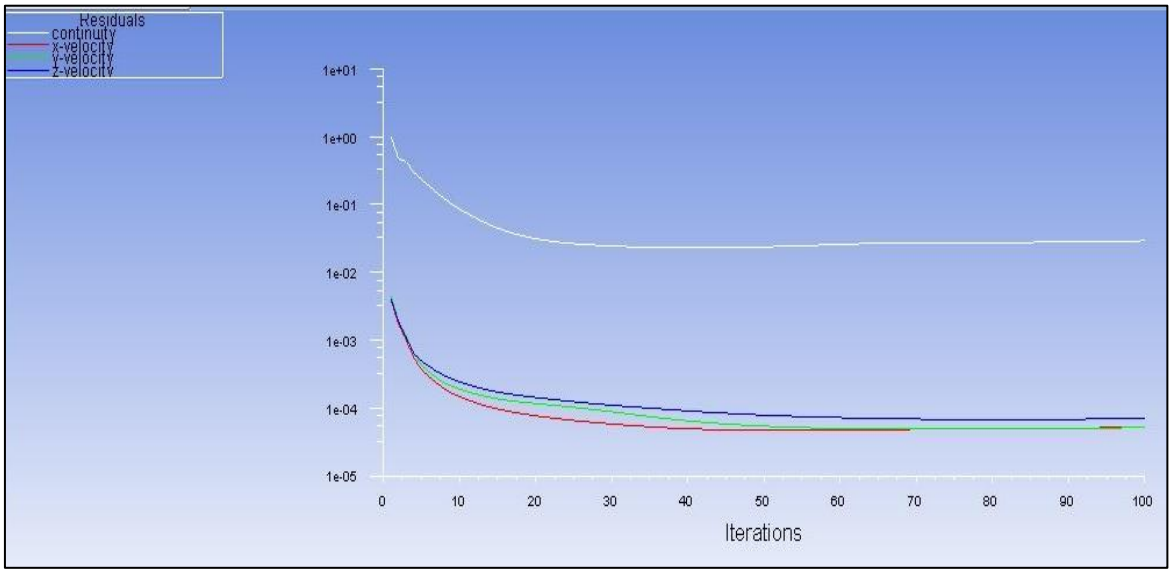
"Başlangıç Değerleri" kullanılan ilk denememizde çarpıklıkların oranı çok fazla olmasına karşın, düğüm ve eleman sayıları oldukça az olduğundan istenilen analiz sonuçlarına ulaşılamamıştır. Çizelge 2.3.deki "Son Değerler" ile işlem tekrarlanmış hassasiyet istenen düzeye çıkarılmıştır.

Boyut fonksiyonu vasıtasıyla eğriliklere bağlı hücre bölünmesi yapılmıştır. Yine aynı şekilde boyutlandırma, düzgünleştirme, hücreler arası geçişler ve hücreler arası açılar analizin hassasiyetini artıracak şekilde ayarlanmıştır. Son mesh işleminin ağ yapısı/kafes yapısı Şekil 2.11'de gösterilmiştir.



Şekil 2.11. Son mesh işleminin ağ yapısı/kafes yapısı

Önceden oluşturulan “isimlendirmeler” üzerinden hava girişi 140 m/s (İHA’lara ait ortalama hava hızı), hava çıkışı 76 cm-hg, uçak yüzeyi ve hava kütle çevresi duvar olarak belirlenmiştir. Müteakiben 100 tekrar (iterasyon) için analiz gerçekleştirilmiştir. Verilen analiz parametre değerleri sonucu x, y ve z yönündeki hızlar ve sürekli (birleşik) hız birlikte türetilmiştir. Analiz sonucunda elde edilen 100 tekrar için analiz işlem sonuçları grafik olarak Şekil 2.12’de tablo olarak Çizelge 2.4’de görülmektedir.

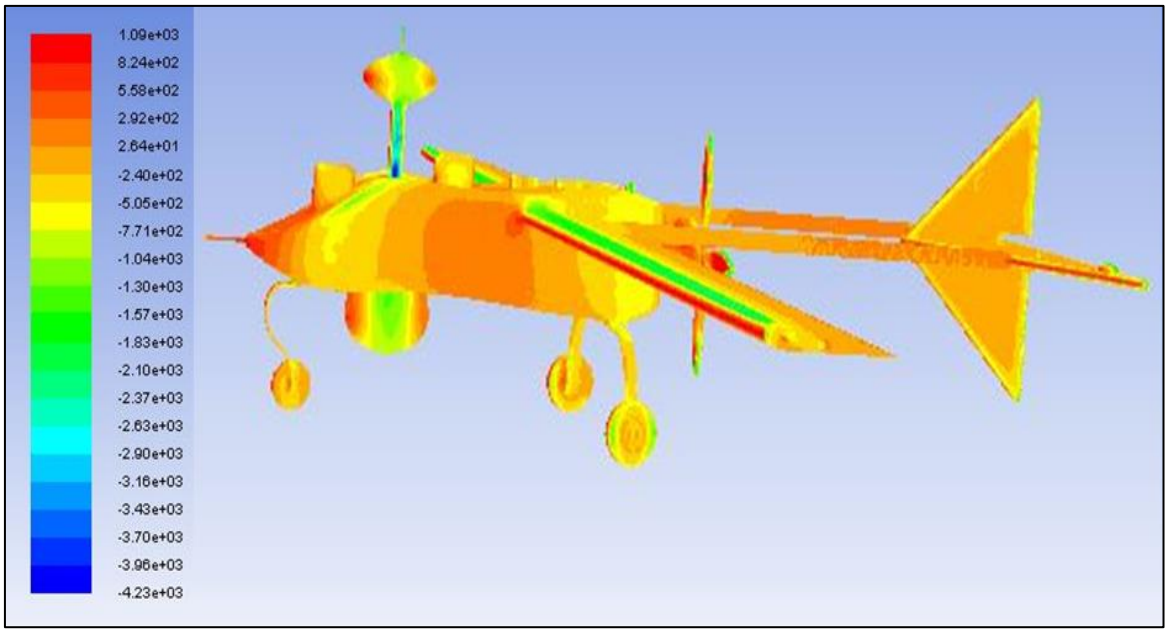


Şekil 2.12. 100 tekrar için analiz işlem sonuçları

Çizelge 2.4. 100 tekrar için analiz işlem sonuçları

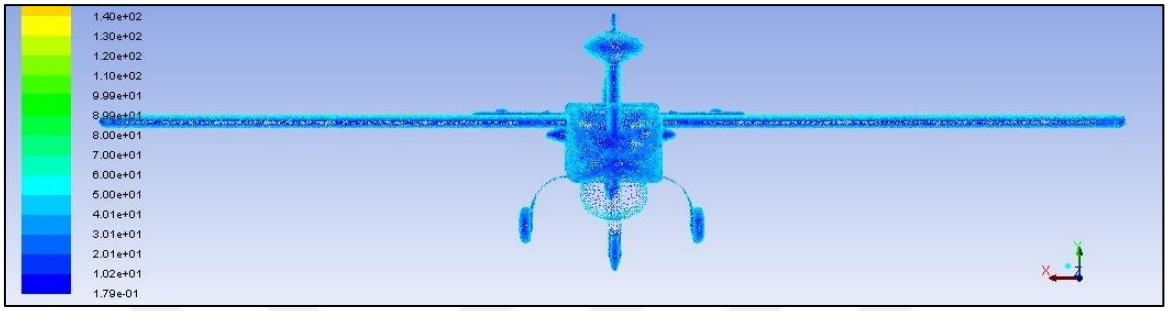
84	2.7763e-02	5.0825e-05	5.0473e-05	6.8830e-05	0:13:32	16
85	2.7816e-02	5.0824e-05	5.0512e-05	6.8845e-05	0:12:39	15
86	2.8044e-02	5.0930e-05	5.0584e-05	6.8792e-05	0:11:47	14
87	2.8134e-02	5.1120e-05	5.0741e-05	6.8854e-05	0:10:58	13
88	2.8257e-02	5.1236e-05	5.0954e-05	6.9020e-05	0:10:03	12
iter	continuity	x-velocity	y-velocity	z-velocity	time/iter	
89	2.8379e-02	5.1416e-05	5.1119e-05	6.9307e-05	0:09:15	11
90	2.8415e-02	5.1470e-05	5.1152e-05	6.9539e-05	0:08:29	10
91	2.8449e-02	5.1573e-05	5.1272e-05	6.9670e-05	0:07:38	9
92	2.8482e-02	5.1755e-05	5.1407e-05	6.9847e-05	0:06:46	8
93	2.8550e-02	5.1914e-05	5.1615e-05	6.9979e-05	0:05:56	7
94	2.8601e-02	5.2026e-05	5.1726e-05	7.0132e-05	0:05:04	6
95	2.8688e-02	5.2155e-05	5.1775e-05	7.0345e-05	0:04:13	5
96	2.8779e-02	5.2270e-05	5.1906e-05	7.0478e-05	0:03:22	4
97	2.9051e-02	5.2401e-05	5.2037e-05	7.0760e-05	0:02:31	3
98	2.9264e-02	5.2647e-05	5.2250e-05	7.0981e-05	0:01:41	2
99	2.9284e-02	5.3004e-05	5.2474e-05	7.1300e-05	0:00:50	1
iter	continuity	x-velocity	y-velocity	z-velocity	time/iter	
100	2.9342e-02	5.3312e-05	5.2624e-05	7.1465e-05	0:00:00	0

İHA yüzeyinde oluşan statik basınçlar ve hız vektörleri elde edilir. Bahse konu statik basınçlar Şekil 2.13'de sunulmuştur. Uçak üzerine farklı değerlerde basınçlar etki etmekte olduğu açıkça görülmektedir. Uçağın burun kısmı, kanat ön kısımları, kamera ve vericinin ön kısmı ile özellikle pervane kırmızı renkli alanlarla gösterilmiştir. Bu alanların 1.090 pascal değerinde olduğu şekilden görülmektedir. Sırasıyla turuncu, yeşil, turkuaz ve mavi renkler negatif basınçlardır. Verilen sıralamayla basınç azalmıştır. Yani bu renklerin olduğu bölgelere havadaki hareketinden ötürü negatif basınçlar etki etmiştir.

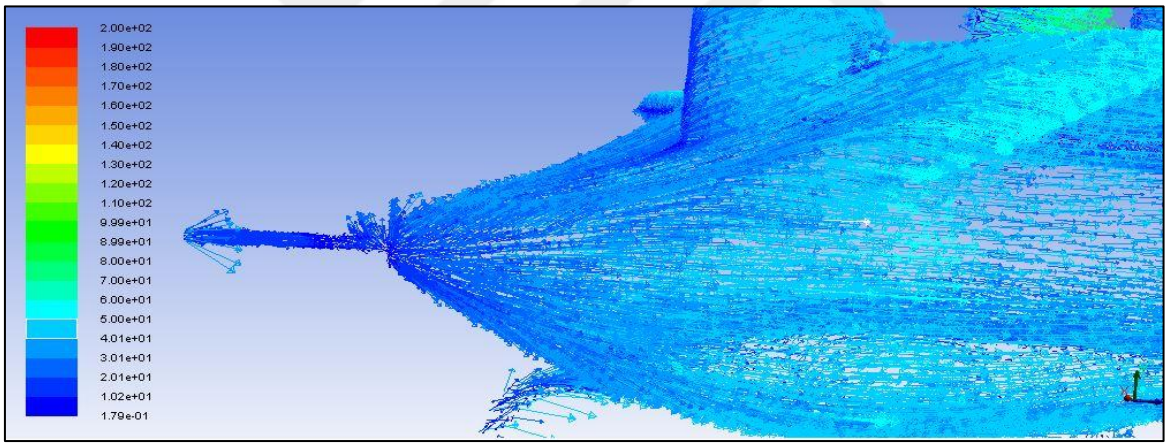


Şekil 2.13. Statik basınç dış hatları

Şekil 2.14 ve 2.15'de renklendirilmiş hız vektörleri gösterilmiştir. Bu analizlerde standart hava şartlarında insansız hava aracına etki eden hava kuvvetleri ve hava akış yönleri tespit edilmiştir. Yine kırmızı ile mavi renkler arasında değişen bu hız vektörleri, havanın akışının hızlı olduğu yerlerden (kırmızı) havanın yavaş olduğu (mavi) hatta türbülans yaşanan bölgelere kadar hava hızlarını göstermektedir.



Şekil 2.14. Renklendirilmiş hız vektörleri-1



Şekil 2.15. Renklendirilmiş hız vektörleri-2

2.7. Analiz Sonucu

Genel olarak uçak analizi çalışmalarında karşılaşılan temel problem, uçağın seyir hızından yüksek hız vektörleri oluşması ve buna bağlı olarak özellikle kanat arka kısımlarında türbülans oluşmasıdır. Bu türbülanslar da uçağın kaldırma kuvvetini azalttığı ve dengesini bozarak meydana getirdiği olumsuz etki sonucu uçak ve uçuş güvenliğini ve emniyetini riske edecek hatta uçağın düşmesine neden olabilecektir.

Sonlu elemanlar metoduyla yapılan akış analizi neticesinde insansız hava aracının 140 m/s gibi yavaş bir hızla uçmasına rağmen uçağın kırmızı renkle gösterilen bölgelerinde 1.090 pascala kadar statik basınçlar görülmüştür. Bu durumda, İHA'nın kat edeceği öngörülen hıza uygun oluşacak yüksek basınç değerlerine göre üretimde önlemler alınmasını gerekmektedir. Diğer yandan, oluşan hız vektörlerinin 17 m/s ile 130 m/s arasında gerçekleştiği tespit edilmiştir. Aynı zamanda uçak etrafında türbülans da gözükmemektedir. Bu tasarıma bağlı uçuş hızının uygun olduğunu göstermekte ve insansız hava aracının daha yüksek hızlarda da uçabileceğine işaret etmektedir.

Özetle bu çalışma sonucunda, tasarlanmış olan 3B modelin yüksek basınçlara maruz kaldığı, malzeme seçiminde bu hususun göz önünde bulundurulması gerektiği, bununla birlikte uçağın yapısının aerodinamik açıdan başarılı olduğu tespit edilmiş ve görülmüştür ki yüksek statik basınç noktaları için önlemler alındığı takdirde tasarlanan insansız hava aracımız güvenli ve uygun aerodinamik yapıya sahiptir.

3. İNSANSIZ HAVA ARAÇLARINDA HABERLEŞME (VERİ LİNKİ)

İHA'larda haberleşme ise genel olarak İHA üzerinde bulunan verilerin yer (kara ve deniz platformları) ve hava sistemlerince izlenebilmesini ve/veya İHA'ların ve ilgili alt sistemlerinin yer ve hava sistemlerince komuta/kontrol edilebilmesi amaçlı belirli verilen ilgili birimlere kablosuz gerçek zamanlı ve/veya gerçek zamana yakın aktaran sistem ve/veya sistemler bütünü olarak tanımlanabilir.

Farklı İHA ve harekât birimlerinin birlikte çalışabilmesini sağlamak amaçlı RF katmanda birbirleriyle konuşabilen standart sistemler kullanılmaya başlanılmıştır. Bu kapsamda Birlikte Çalışabilirlik adı altında NATO çerçevesinde veri linkleri ile ilgili çalışmalar yapılarak STANAG 7085 (Interoperable Data Links) dokümanı oluşturulmuştur.

3.1. İHA'larda Haberleşme Sistemleri

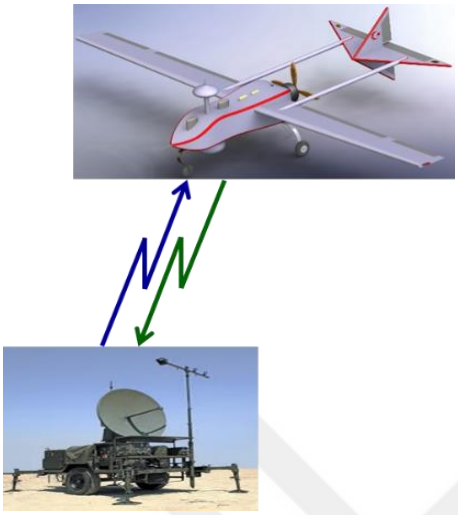
Görüş Hattı Veri Haberleşmesi (LOS - Line of Sight), Görüş Hattı Ötesi Veri Haberleşmesi (BLOS - Beyond Line of Sight) ve Taktik Veri Haberleşmesi olarak üç ana kategori de sınıflandırılabilir.

3.1.1. Line of sight

Şekil 3.1'de sunulan line of sight (LOS) noktadan-noktaya yüksek veri hızında haberleşme sağlayan sistemlerle sağlanır. Kullanım amaçları İHA'ların veri aktarımını, görüş hattı içerisinde kalan diğer noktalar ile sağlamaktır. Görüş Hattı Veri Haberleşmesi için değişik bantlarda çalışan sistemler bulunmaktadır. Öne çıkan sistemlerin C-Bant ve Ku-Bant'da oldukları görülmektedir. Yüksek veri aktarım kapasiteleri sayesinde yüksek yoğunlukta veri çıktısı sağlayan faydalı yük verilerinin görüş hattı içerisinde bulunan diğer noktalara aktarımı kolaylıkla yapılabilir. 274 Mbit/s seviyelerinde veri aktarım hızına sahip olabilirler.

Yer Birimi ve Hava birimi olmak üzere iki bölümden oluşurlar. Yüksek veri hızlarına ulaşılabilmesi için hem hava aracında hem de yer sisteminde takip (yönlendirilmiş) antenlerine ihtiyaç duyulur. Bu tip sistemlerin, çalışma mesafesini alıcı-verici cihazlarına

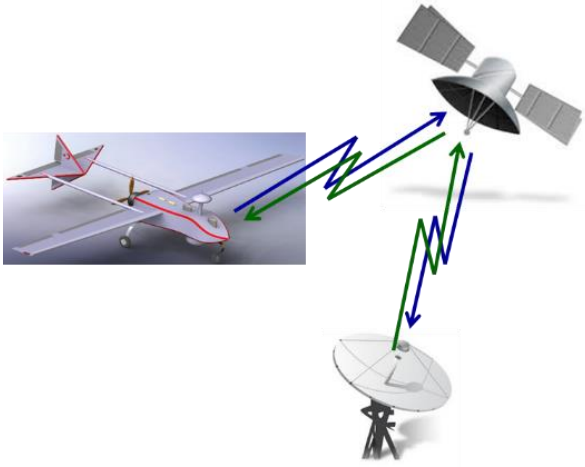
bağlı olarak ortalama 200-250 km civarındadır. Çalışma mesafesi artırmak için Röle Haberleşme Sistemleri kullanılır.



Şekil 3.1. LOS

3.1.2. Beyond line of sight

Diğer ismi ile Uydu Haberleşmesi hava aracının haberleşme ve faydalı yük verilerinin iletim alanını arttırmak ve görüş hattı veri iletim zorunluluğunu ortadan kaldırmak için kullanılabilecek bir haberleşme biçimidir. Dünya ile uzay arasında doğrudan görüş hattı olduğundan, uydu haberleşmesi uzak mesafeler ile en kolay mikrodalga haberleşme şeklidir. Beyond line of sight (BLOS) Şekil 3.2'deki gibi yörüngedeki iletişim uydularıyla sağlanmaktadır.



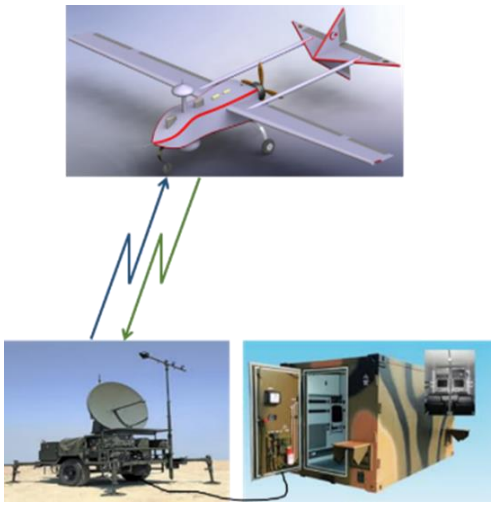
Şekil 3.2. BLOS

3.1.3. Taktik veri haberleşmesi

İHA görev alanlarını destekleyen, birden çok İHA ve hava aracı ve yer sistemlerin eş zamanlı haberleşmesini sağlayan, ağ merkezli harekâtı destekleyen, yakın ağların aynı operasyon ortamında birbirini engellemeden çalışabilmesini düzenleyen, güvenli veri aktarım özelliklerim içeren sistem olarak tanımlanabilirler. Taktik Veri Haberleşme Sistemi deyince ilk olarak Link-16 Müşterek Taktik Data Link Sistemi akla gelmektedir. Bilindiği gibi Link-16 Ağ Destekli/Merkezli Yetenek altyapısının temelini oluşturmaktadır. Link-16 veri aktarımında düşük bant genişliğine sahiptir [33].

3.2. İHA'nın ve Faydalı Yükün Komuta Edilme Mantığı

YKİ'den verilen komutların YVT vasıtasıyla İHA'ya gönderilmesi; İHA'dan alınan telemetre (uçuş verileri) ile faydalı yükten alınan video bilgilerinin de ters istikamette yine YVT üzerinden YKİ'ye gönderilmesi mantığıyla çalışan bir sistemdir. İHA-YVT arasında kablosuz, YVT-YKİ arasında ise kablolu haberleşme sistemi mevcuttur. Faydalı yük komuta mantığı Şekil 3.3 ile gösterilmiştir.

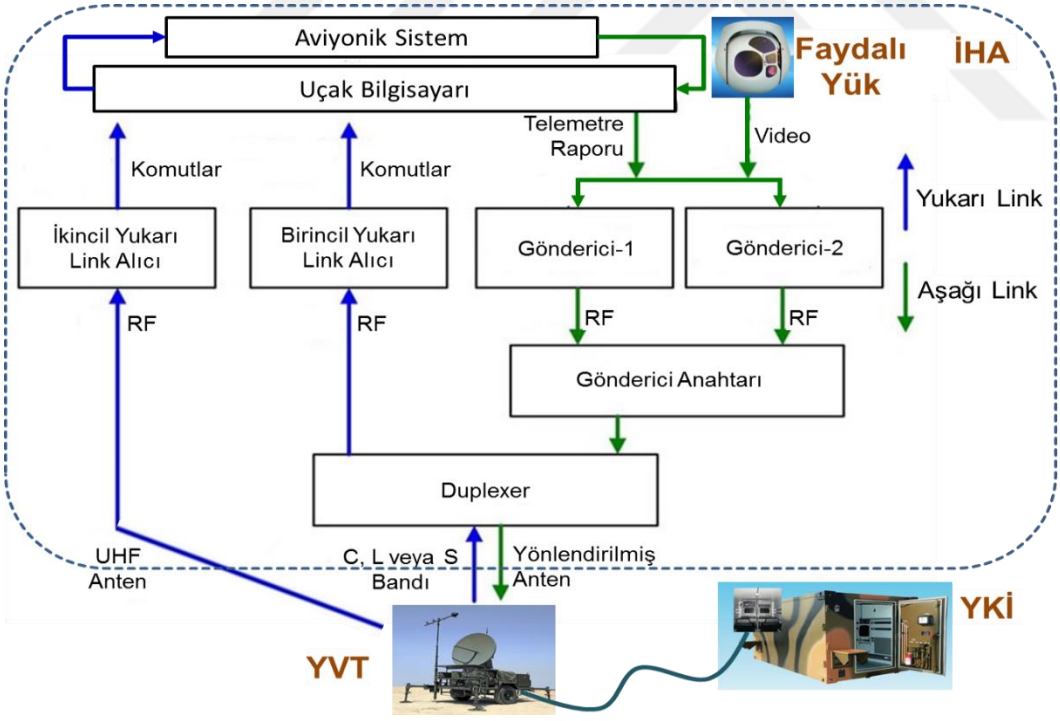


Şekil 3.3. Faydalı yük komuta mantığı

3.3. İHA Veri Linki Sistemi

İHAS'da iki yukarı link (UHF ve C/L/S/Q), bir aşağı link (C/L/S/Q) bulunmaktadır. Bunun nedeni; aşağı linkte problem yaşansa bile hava aracının yönlendirilebilmesi, yukarı linkte

problem yaşanması durumunda ise hava aracının kontrolünün kaybedilmesidir. Dolayısı ile yukarı link daha önemli olduğundan iki ayrı bant üzerinden eş zamanlı olarak yayım yapılmaktadır ve C/L/S/Q bant linki ana linktir. Pilot ve faydalı yük operatörünün verdiği komutlar YKİ'den kablo vasıtası ile YVT'ye iletilmekte oradan da yukarıda bahsettiğimiz gibi iki ayrı göndermeç vasıtasıyla UHF ve C/L/S/Q bant üzerinden kablosuz olarak yayımlanmakta; bu sinyaller de İHA üzerinde bulunan yine iki ayrı almaç tarafından alınarak hava aracında bulunan bilgisayara (aviyonik sistemler) gönderilmektedir. Bilgisayar aldığı komutlara göre hava aracını ve üzerindeki faydalı yükü kontrol etmekte, neticesinde oluşan video görüntüsü ve telemetre (uçuş verileri) bilgileri C/L/S/Q bant üzerinden yedekli göndermeç vasıtasıyla YVT'ye oradan da kablolu olarak YKİ'ye gönderilmektedir. Hava aracında bir C/L/S/Q bant anteni bulunduğu ve alma/gönderme işlemi bu anten üzerinden yapıldığı için duplexer (alıcı-verici) cihazıyla sırası ile alma ve gönderme işlemleri tek anten üzerinden yapılabilmektedir. İHAS veri linki sistemi şematik olarak Şekil 3.4'de sunulmuştur.



Şekil 3.4. İHAS veri linki sistemi

Hem YVT'de hem de hava aracında C/L/S/Q bant için alternatifli çalışan ikişer ayrı anten bulunmaktadır. Bunlar; çubuk anten (Omni) ve yönlendirilmiş anten (ADA/Dir/Dish)'dir. İHA-YVT arasında link, görüş hattı (LOS) esasına göre çalışmaktadır. İniş ve kalkışlarda

antenler arası mesafe kısa olduğundan antenlerin takip zorluğu olmaması için menzili daha kısa olmakla birlikte yönlendirme sorunu bulunmayan Omni anteni tercih edilmesi, antenler arası mesafe arttıkça da menzili daha uzun olan ADA anten kullanılması hal tarzı olarak belirlenmiştir. Anten değişimi pilot tarafından manuel olarak yapılmaktadır. İHA ve YVT üzerinde bulunan GPS'ler vasıtası ile sistem tarafından koordinatlara uygun olarak matematiksel hesap yapılmakta ve antenler hesaplanan açılara uygun olarak birbirlerine dönmektedir. Seçilen antene göre veri linki mesafeleri kilometre cinsinden Çizelge 3.1'de sunulmuştur.

Çizelge 3.1. Seçilen antene göre veri linki mesafeleri

			YVT		
			C/L/S/Q		UHF
			Yön. Anten	Çubuk Anten	
İHA	C/L/S/Q	Yön. Anten	150-200	3-5 km.	-
		Çubuk Anten	150-200	3-5 km.	-
	UHF		-	-	150-180

3.4. İHA'larda Yaygın Olarak Kullanılan Hava Frekans Bantları

İHAS'larda veri iletişimi öncelikle RF uygulamaları ile gerçekleştirilmektedir. Genellikle uydu haberleşme sistemi ve görüş hattı sistemi tercih edilmektedir. Bu maksatla İHA'larda yaygın olarak kullanılan hava frekans bantları aşağıda, özetle Çizelge 3.2'de sunulmuştur.

Çizelge 3.2. İHA'larda yaygın olarak kullanılan hava frekans bantları

Bant	Frekans
HF	3-30 MHz
VHF	30-300 MHz
UHF	300-1000 MHz
L	1-2 GHz (General) 950-1450 MHz (IEEE)
S	2-4 GHz
C	4-8 GHz
X	8-12 GHz
Ku	12-18 GHz
K	18-26,5 GHz
Ka	26,5-40 GHz

3.4.1. Ku bant

Tarihsel olarak yüksek hızlı bağlantılar için kullanılmaktadır. Kısa dalga boyları ve yüksek frekanstan kaynaklanan yayılma fazlalığı nedeniyle veri kayıplarından mustariptir. Ancak aynı zamanda birçok engelin içerisinden geçebildiği için büyük miktarda veriyi taşıyabilmektedir.

3.4.2. K bant

Büyük miktarda veri taşıyan geniş frekans aralığına sahiptir. Güçlü vericiler gerektirmesi ve çevreden müdahalelere duyarlı olması dezavantajlı taraflarıdır.

3.4.3. S ve L bant

500 Kbps üzerinde iletim hızları olan veri bağlantılarına müsaade etmezler. Büyük dalga boyuna sahip sinyalleri engellere nüfuz edebilir ve vericileri K bandı vericilerinden daha az güç gerektirirler.

3.4.4. C bant

Göreceli daha büyük iletim/alım antenine ihtiyaç duymaktadır. Bu frekanslar bulut veya yağmur gibi meteorolojik oluşumlardan çok az etkilenirler ve bu sayede çok uzun menzillere ulaşmak mümkün olur.

3.4.5. X bant

X bandı elektromanyetik spektrumun mikrodalga telsiz bölgesinin bir parçasıdır. Askeri maksatlar için tahsis edilmiştir [34]. Bu nedenle askeri telsiz iletişimi için frekans bantlarını ayırmaya zorunluluğu yoktur.

3.5. Hava Veri Linki Zorlukları

Havacılıkta kullanılan veri linklerinin tasarımı diğer kablosuz linklere kıyasla daha zordur. Temel zorluklar şunlardır: uzun mesafe, yüksek hız ve spektrum.

- Veri iletiminin uzun mesafeli yapılması önemli güç kaybına ve çok düşük spektral verimliliği neden olmaktadır.
- Uçakların yüksek hızları yüksek Doppler yayılması oluşturarak spektral verimliliği olumsuz etkilemektedir.
- Havacılık iletişim/haberleşme sistemleri genel olarak yüksek frekans (HF) ve çok yüksek frekans (VHF) bantları ile uydu haberleşme sistemlerini kullanmaktadır. Bununla birlikte; uydu haberleşme sistemleri uçuşun tüm bölümlerinde kullanılabilir değil, HF ve VHF frekansları da yetersiz kalmaktadır. Artan İHAS hava trafiği de göz önünde bulundurulduğunda hava-yer veri iletimi için yeni spektrum belirlenmesi ihtiyacı hâsıl olmuştur [35].

3.6. Genel Frekans Planlama ve Tahsis Kriterleri

Elektromanyetik dalgalar yoluyla haberleşme yapılabilmesi ve elektromanyetik dalgaların birbirini bozmadan kullanılabilmesi için frekans planlamasına gerek duyulmaktadır. Frekans spektrumunun planlaması ve belirli hizmetlerde (kara, hava, deniz, uydu vb.) değişik amaçlar için kullanımı; üyesi bulunduğumuz Uluslararası Telekomünikasyon Birliği (International Telecommunication Union-ITU) tarafından belirlenen Telsiz Tüzüğü (Radio Regulation-RR) ile Avrupa Posta ve Telekomünikasyon Komisyonu (Commission of European Post and Telecommunications-CEPT) karar ve tavsiye kararları çerçevesinde milli frekans planı yapılarak uygulanmaktadır. Ayrıca Uluslararası Sivil Havacılık Örgütü (International Civil Aviation Organization-ICAO) ve Uluslararası Denizcilik Örgütü (International Maritime Organization-IMO) gibi ilgili kuruluşların ITU nezdinde koordineli çalışmaları sonucu oluşturulan esaslar da dikkate alınmaktadır. Belirtilen uluslararası kuruluşlar, hazırladıkları planlamalarda karıştırmaya (enterferans) neden olmadan, frekansların verimli kullanımını sağlamayı amaçlamaktadırlar. Değişik hizmetler için yapılan yeni frekans planlama raporları belirli aralıklarla yapılan uluslararası toplantılarda ülke değerlendirmelerine sunulur. Üye ülkelerin görüşleri ve önerileri doğrultusunda son halini alan planlamalar yayımlanarak uygulamaya konulur. Daha sonra ülkeler yapılan genel planlamaya göre kendi milli frekans planlamalarını yaparak gerekli frekans tahsislerini yaparlar [24].

Ülkemizde ise; haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması,

kaynakların etkin ve verimli kullanılması, haberleşme alt yapı, şebeke ve hizmet alanında teknolojik gelişimin ve yeni yatırımların teşvik edilmesi ve bunlara ilişkin usul ve esasların belirlenmesi amacıyla 05.11.2008 tarihinde Elektronik Haberleşme Kanunun (EHK) yayımlanmıştır.

3.6.1. Bilgi Teknolojileri Kurumunun (BTK) görevleri

Madde 6 (f) bendi Elektronik haberleşme hizmetlerinin sunulması ve elektronik haberleşme şebeke ve altyapılarının tesis ve işletilmesi için gerekli olan frekans, uydu pozisyonu ve numaralandırma planlamasını ve tahsisini yapmak,

Madde 6 (m) bendi Frekans planlama, tahsis ve tescil işlemlerini, güç ve yayın sürelerini de göz önünde tutarak uluslararası kuruluşlarla işbirliği de yapmak suretiyle yürütmektir.

3.6.2. Frekans planlama, tahsis ve tescili ile ilgili olarak, Madde 36

Telsiz yayınlarının birbirleri üzerinde elektromanyetik girişim oluşturmaması ve frekans bantlarının etkin ve verimli şekilde kullanılmasını sağlamak amacıyla uluslararası frekans planlaması ve uluslararası kuruluşların aldığı kararlar da dikkate alınarak milli frekans planlaması, tahsisi, uluslararası koordinasyon ile tescil işlemleri Kurum tarafından yapılır ve uygulanır. Frekans tahsislerinde Dışişleri Bakanlığı, Jandarma Genel Komutanlığı ile Sahil Güvenlik Komutanlığı ihtiyaçları da dâhil TSK, Millî İstihbarat Teşkilatı Müsteşarlığına ve Emniyet Genel Müdürlüğüne öncelik tanınır.

3.6.3. Sahil telsiz istasyonları, deniz ve hava bandı telsiz sistemleri ile ilgili olarak, Madde 42 2. fıkrası

Her çeşit deniz ve hava bandı telsiz haberleşme sistemlerini ve sahil telsiz istasyonları üzerinden yapılan seyir güvenliği haberleşmesi dâhil telsiz haberleşme sistemlerini kurma, kurdurma, kullanma izinlerini verme, ruhsatlandırma, deniz bandı telsiz haberleşme ve seyrüsefer cihazlarına çağrı kodu ve benzeri tahsis ve tescil işlemleri Telsiz İşletme Müdürlüğünce yürütülür [36].

3.6.4. Deniz ve hava bandı frekans tahsisi

EHK'nın yukarıda belirtilen kanun maddeleri gereği, her türlü sistem için frekans planlaması, tahsisi ve uluslararası koordinasyon işlemleri BTK tarafından yapılır iken, deniz ve hava bandı telsiz haberleşme sistemi kurma ve kullanma izni ve ruhsatname işlemleri Kıyı Emniyeti Genel Müdürlüğü (KEGM) Telsiz İşletme Müdürlüğüne devredilmiştir. İHA'lar için uluslararası frekans planlaması ve uluslararası kuruluşların aldığı kararlar da dikkate alınarak yapılacak milli frekans planı, frekans tahsisi, uluslararası koordinasyon ile tescil işlemleri BTK tarafından yapılacak, sistem kurma/kullanma ve ruhsatlandırma işlemleri ise KEGM Telsiz İşletme Müdürlüğünce yapılacaktır. Hava ve deniz telsiz sistemleri dışında kalan telsiz sistemleri ile ilgili frekans tahsisi, tescili ve ruhsatlandırma işlemleri BTK tarafından yürütülmektedir. Yine yukarıda belirtilen yasal düzenlemelere istinaden Türkiye'de İHA üreten şirketlerin frekans talepleri BTK tarafından değerlendirilmekte, UHF bandında veya talep edilen diğer bantlarda geçici tahsisler yapılmaktadır.

Ar-Ge faaliyetleri için tasarlanacak model uçak ve benzeri hava araçları için ülkemizde serbest kullanıma açık frekanslar bulunmaktadır. Bu frekanslar, BTK tarafından yayımlanan, Kısa Mesafe Erişimli Telsiz (KET) Cihazları Yönetmeliğinin 13. maddesinde, 34.995-35.225 MHz bandı olarak belirtilmiştir [24].

3.7. Veri Linki Güvenliği

Uçak sistemlerinin ve görevin izlenmesi ve uçağın manuel kontrolü için, veri linki bağlantısı gerekmektedir. Veri linki; elektromanyetik karıştırmaya açık olmak, fiziksel mesafe, sinyalin gücü, sinyali etkileyen fiziksel engeller, eldeki bant genişliği ve sadece tahsis edilmiş frekansların kullanılabilmesi limitlerini içerir. Bu konuyu incelerken veri linklerini öncelikle kablolu ve kablosuz olarak ayırmakta fayda mütalaa edilmektedir.

3.7.1. Kablosuz veri linki

Sistemde iki yukarı ve bir aşağı link olduğu, linklere birden fazla şekilde müdahale edebileceği göz önünde bulundurulduğunda dışarıdan yapılacak bir etki ile;

- Yukarı linkler bastırılarak/karıştırılarak İHA'nın tarafımızdan kontrolü engellenebileceği,
- Yukarı linkler daha güçlü bir sinyalle ele geçirilerek İHA'nın düşman tarafından kontrolü sağlanabileceği,
- Aşağı link bastırılarak/karıştırılarak İHA'dan telemetre ve video bilgilerinin tarafımızdan alınması engellenebileceği,
- Aşağı linke girilerek İHA'dan gelen telemetre ve video bilgileri bilgimiz dışında düşman tarafından ele geçirilebileceği,
- Aşağı link yerine başka bir yayın yapılarak tarafımıza yanlış bilgi gönderilebileceği,
- Bu işlemlerin kasıtlı olarak yapılabileceği gibi bölgede uçuş yapan başka İHA'lara ait veya ortamda bulunan diğer sinyallerle de sağlanabileceği değerlendirilmektedir.

3.7.2. Kablolu veri linki

Kablolu veri linklerine fiziksel olarak girdi yapılması gerekmektedir. Fakat İHAS'larda kablolu veri linki, YKİ-YVT arasında kısa mesafeli kullanıldığından bu ihtimalin göz ardı edilebileceği değerlendirilmektedir.

3.8. Radyo Frekans (RF) Haberleşme: Sinyali Yayılma Özellikleri

Radyo frekansı yayıncılıkta bir bilgi sinyali ile modüle edilmiş olan taşıyıcı sinyal anlamına gelir. Alınan Sinyal Gücü (Received Signal Strength-RSS), vericinin gönderdiği sinyalin alıcıya ulaştığı zamanki gücü hesaplanarak aradaki mesafenin tahmini hakkında bilgi vermektedir. Friis'in Eş. 3.1'deki formülüne göre RSS:

$$Pr = Pt - PL(d) + Gr + Gt \quad (3.1)$$

Pr alınan sinyalin gücü (dBm), Pt sinyalin yayımlandığı gücü (dBm), PL(d) yol kaybı (dB), Gr ve Gt ise alıcı-verici anten kazanımlarıdır.

Dolayısı ile RSS; alıcı-verici anten tipi, antenlerin yönlendirilmesi, yayım gücü ve yol kaybından etkilenmektedir [37].

3.9. Sinyal Ortamı (Signal Environment)

Sinyal ortamı alıcı tarafından kapsanan frekans aralığı içinde o alıcının antenine ulaşan tüm sinyalleri kapsamaktadır. Ortam sadece kendi sinyallerimizi değil, tehdit sinyalleri, tarafsız sinyalleri, diğer dost sinyallerini de içermektedir. Çoğu dost veya tarafsız sinyal olsa da alıcı sistemi, dost sinyalleri ayırt ederek gereksiz sinyalleri elimine etmeli ve düşman sinyalleri de tespit edebilmelidir. Zaten yoğun olan sinyal ortamı her geçen gün daha da yoğunlaşmaktadır.

3.9.1. Açısal kapsam (angular coverage)

Gemiler ve karada konuşlu EH sistemleri için yatayda 360 derece düşey de ise 10-30 derece arası açısal kapsama alanıdır. Hava taşıtlarındaki alıcılar karada konuşlu alıcılara kıyasla daha geniş kapsama alanına sahiptir.

3.9.2. Kanal doluluğu (channel occupancy)

Modern savaş mobil sistem yoğunluklu olduğundan iletişim çoğunlukla kablosuz sistemler üzerine kurulmuştur. Bu da büyük miktarda ses ve veri linkini kapsamaktadır. Taktik haberleşme ortamının kanal doluluğu % 10 olarak kabul edilmektedir. Ancak bu değer yanıltıcı olabilmektedir; kanalların tek tek incelenmesi durumunda oranın % 100'e yaklaştığı kolayca görülebilmektedir. Birçok sinyalin varlığı bulundu sinyaller üzerinde hızlı arama yapan daha ve ayrıntılı analiz için duraklamalar yapan herhangi bir yaklaşım üzerinde önemli bir etkiye sahiptir.

3.9.3. Duyarlık (sensitivity)

Sinyal yoğunluğunu tespit etmede önemli hususlardan biri de alıcının duyarlığıdır. Alınan sinyalin gücü alıcı-verici mesafesinin karesi oranında azalmaktadır.

Alıcı duyarlığı gerekli bilginin alınabileceği en zayıf sinyal olarak tanımlanabilir. Düşük duyarlıklı alıcı ve düşük kazanımlı antenden oluşan sistemler yüksek duyarlıklı alıcı ve yüksek kazanımlı antenden oluşan sitemlere oranla daha az sinyale maruz kalmaktadır. Bu

durum düşman vericilerin tespitinde değerlendirilmesi gereken toplam sinyal miktarını azaltarak arama sorununu kolaylaştırmaktadır [38].

3.10. Yaygın Olarak Kullanılan Anten Performans Parametreleri

Yaygın olarak kullanılan anten performans parametreleri; kazanç, frekans kapsama alanı, bant genişliği, polarizasyon, sinyal genişliği ve verimdir. Kazanç (gain), sinyalin anten tarafından edinilmesine paralel olarak sinyal kuvvetinde meydana gelen artıştır. Genellikle dB cinsinden gösterilmektedir. Pozitif veya negatif de olabilir. Frekans kapsama alanı (frequency coverage) antenin sinyali uygun performans parametreleri ile alabileceği ya da yayımlayabileceği frekans mesafesidir. Bant genişliği (bandwidth) frekans birimlerinde antenin frekans aralığıdır. Genellikle yüzde bant genişliği açısından belirtilmiştir. Polarizasyon/kutuplaşma (polarization), dalgaların iletildiği veya alındığı yöndür. Dikey, yatay, saat istikameti veya tersi istikamette vb. olabilir. Sinyal genişliği (beamwidth) antenin açısal kapsama alanıdır. Sinyal genişliği genellikle (her zaman değil) derece ve yatay düzlem için ifade edilir. Verim (efficiency) ise yönlülük için kazanç oranıdır [38]. Bir başka değişle, antene gelen gücün anten tarafından yayılan güce göreceli oranıdır. Düşük verimlilikteki anten sinyal gücünün bir kısmını alamadan yansıtır bir kısmını da anten içerisinde kaybeder.

3.11. İletişim Sistemi Gürültüsü (Noise)

Gürültü, elektrikli sistemleri etkileyen istenmeyen sinyallerdir. Gürültünün sinyal üzerindeki varlığı sinyali engeller ya da maskeler; alıcının kabiliyetini bastırır böylece doğru verinin aktarılmasını önler. Hem insan kaynaklı hem de doğal nedenlerden oluşabilir. İnsan kaynaklı; buji ateşlemesi ve diğer elektromanyetik sinyaller, doğal nedenler ise; atmosfer, güneş ve diğer galaksi ile ilgili olaylardır. Ancak ince mühendislikle titiz tasarlanmış sistemler gürültünün çoğunu filtreleme, kalkan/koruma, modülasyon ve uygun alıcı konumu seçimi ile eleyebilir [39].

3.12. Sinyal Arama Stratejisi

Genel olarak şu üç metottan biri kullanılmaktadır: Genel arama (General Search), yönlendirilmiş arama (Directed Search) ve sıralı yeterlik (Sequential qualification).

3.12.1. Genel arama

Sinyale ilişkin hiçbir ön bilgi bulunmamaktadır. Her frekans ve sinyal istikameti tercih veya öncelik olmadan araştırılır. Genel aramanın son ürünü; sonraki daha gelişmiş aramaya veya keşfedilen önemli düşman varlıklarına karşı doğrudan müdahaleye imkân tanıyan çevrenin "haritası"dır.

3.12.2. Yönlendirilmiş arama

Çevreyi bilmenin getirdiği avantaja sahiptir. Birçok sinyalin frekansı, modülasyon ve önceliğini hatta küçük ölçekli alıcı sistemlerinde dahi depolamak için pratiktir. Önemli frekanslara yönelik bilgiler hafızadan çağrılarak tekrar sorgulama yapılabilir. İlgi alanında olmayan frekans ve bölgeler atlanarak zaman kazanılabilir.

3.12.3. Sıralı yeterlik

Bulunan herhangi bir sinyalin bazı parametrelerinin pratik ölçümünü içerir; böylece öncelikler doğrultusunda yayım parametrelerini incelemek için daha çok vakit ayrılmasına gerek olup olmadığına karar verilebilir. Genel olarak az zamana ihtiyaç duyan parametreler ilk sıralamanın yapıldığı parametrelerdir. En yaygın yaklaşım ilk olarak herhangi bir sinyal enerjisi için belirlenmiş öncelikli frekans aralığını araştırmaktır. Bu her kanal için mikro saniyelerle ifade edilebilir. Enerji bulununca ikinci adımda sıradaki parametre olan modülasyon incelenir. Modülasyon spektral analiz ile kolayca bulunabilir [38].

3.13. RF - Yön Bulma (Direction Finding - DF)

Vericinin istikametini belirleme işlemidir. Yön bulma, hem askeri hem sivil maksatlı kullanımlarda sinyalin kaynağının yerinin tespiti ve sinyalin izlenebilmesi açısından önemlidir. Elektronik Harp (EH) ve Sinyal İstihbarat (SİNİS) sistemleri de vericinin yerinin tespit edilmesine ihtiyaç duymaktadır. Konumun bulunabilmesi için öncelikle sinyalin alıcıya ulaşım açısının belirlenmesi gerekmektedir. Yön bulma; seyrü sefer, askeri istihbarat, mobil haberleşme, acil durum aramaları, coğrafi konumlama, sonar, deprembilim, arama-kurtarma, astronomi, halk güvenliği, çevre izleme ve haberleşme istihbaratı alanlarında geniş uygulama alanın sahiptir [40]. Yön bulmanın maksadı vericinin konumunu birden çok

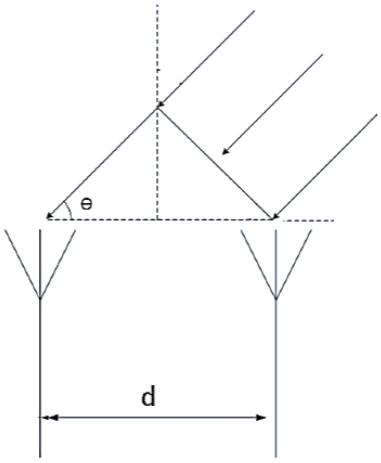
alıcıdan edinilen veriler ile hesaplama sonucu tespit etmektir. Bu süreçte göz önünde bulundurulması gereken birçok husus vardır: antenlerin ve konumlarının seçimi, alıcının yapısı ve optimum algoritma. Yön bulma tekniklerinde çoklu antenler değişik geometrik konfigürasyonlarda yerleştirilebilmektedir. Çoğu dizilimlerde kullanılan elementler aynıdır. En yaygın kullanılan geometrik şekil düz veya dairesel hattır. Düz hattın dezavantajı tüm hat boyunca eşit çözünürlük kapasitesine sahip olmamasıdır. Bu dezavantaj dairesel dizilimde bulunmamakta, 360 derece eşit çözünürlüklü kapsama sağlanabilmektedir [41]. Herhangi bir yönden gelen RF sinyalinin istikametini belirlemek için omni (360 derece) arama yapılması gerekmektedir. Sonuç olarak bunu sağlayabilmek için en sık başvurulan yöntem dairesel anten dizilimidir [42].

RF sinyalleri kaynağının pozisyonu hakkında bilgileri de içermektedir. Bu bilgiye ulaşmak için kullanılan çeşitli yöntemler ve çeşitli sınıflandırmalar vardır. Bazıları, yöntemleri klasik-modern diye ayırırken bazıları deterministik-olasılıklı diye ayırmakta, diğer bir grup da hassasiyetlerine göre tasnif etmektedir.

3.13.1. Genel tasnifler

Faz karşılaştırma (phase comparison)

Dalga yayılımının doğası gereği, farklı elemanlara ulaşmaları farklı zamanlar alabilmektedir. Şekil 3.5'de görüldüğü gibi iki sıralı antene dalganın ulaşması belli bir açı ve açıya bağlı olarak zaman farkı ile gerçekleşmektedir.



Şekil 3.5. İki sıralı antene dalganın ulaşması

Eş. 3.2'de $\Delta\phi$ faz farkı, k yayılma sabiti, d antenler arası mesafe ve θ gelen sinyal ve antenlerin oluşturduğu istikamet arası açıyı göstermektedir. k ve d sabit olduğundan faz farkı θ açısının bir fonksiyonudur [42].

$$\Delta\phi=k.d.\cos(\theta) \quad (3.2.)$$

Genlik karşılaştırma (amplitude comparison)

Her dizi elemanı/anteni üzerine gelen sinyal gücü, RF kaynağının anten dizisine uzak olduğu alanda aynı alınmaktadır. Her eleman tarafından alınan sinyal güçlerinin farklılığı elemanların radyasyon paternlerinden kaynaklanmaktadır. İşlem sırası şöyledir:

- Radyasyon paternleri ölçülür ve değerler bir tablo haline getirilir.
- Bu tablolar, elemanlardan alınan sinyal gücü ve karşılık gelen sinyal varış açısı (Angel of Arrival) oranlarını kapsar.
- Alınan sinyal gücü (RSS) ile tablodaki güçler karşılaştırılır.
- Birbirine en yakın olan veri seti tahmini ulaşma açısıdır.

Genlik karşılaştırmada antenler, sıralı antenlerin radyasyon paternlerine uygun olarak düzenlenir. Bu da her istikamette sinyal arama yeteneği demektir [42].

Deterministik

Alınan sinyal gücü göstergesinin (Received Signal Strength Indicator-RSSI) olasılıklı davranışlarını göz ardı eder. Ayrıca hedefin ilk konumu hakkında da ön bilgi bulunmamaktadır.

Olasılıklı (probabilistic)

Bu metot; RF sinyalinin yayılımını % 100 doğrulukla tanımlamanın mümkün olmadığı ve olasılıkların da hesaplamalara dâhil edilmesi gerektiği esasına dayanaktadır. Dolayısı ile alınan sinyal gücü ve mesafe ilişkisi deterministik değildir. Olasılıklı metot bu belirsizlikler ve ölçümlerde oluşabilecek hatalara karşı çözüm getirme amacındadır. Benzer şekilde

vericinin ön konum bilgisi ile de ilgilenmektedir. Bayes dağılımına uygun olarak sonuçları ilgi alanı üzerinde değerlendirir [37].

Orta hassasiyetli teknikler (moderate accuracy techniques)

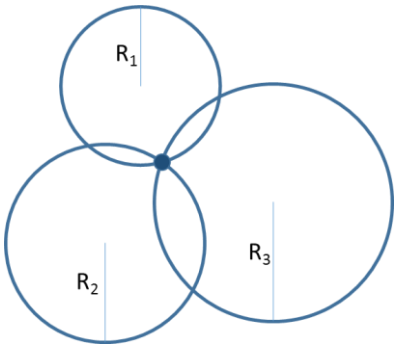
Bu sistemlerin kendileri de göreceli küçük, hafif ve ucuzdurlar. Yüksek hassasiyet beklentisi küçük ölçekli bu tür sistemler için büyük bir problem teşkil etmektedir. Ancak teknolojinin gelişimi ile birlikte ataletsel ölçü birimleri (IMUs) yön bulma sistemleri için yeterli konum ve açı bilgisini sağlayabilmektedir [38].

Yüksek hassasiyetli teknikler (high accuracy techniques)

Genel olarak enterferometre yön bulma tekniğini kapsamaktadır. Uygun kalibre edilmesi durumunda 1° dereceye kadar doğrulukla yön tespit edebilmektedir. Bu teknikle sadece sinyalin erişim açısı tespit edilebilir. Tek Sıra Enterferometre (Single Baseline Interferometer), Çok Sıralı Hassas Enterferometre (Multiple Baseline Precision Interferometer) ve Bağıntılı Enterferometre (Correlative Interferometer) olmak üzere üç gruba ayrılmaktadır [38].

Geometri (lateration) metodu

Şekil 3.6'da gösterildiği gibi en az üç ayrı konumdaki referans noktasından istifade ile konum değerlendirmesi yapılmaktadır. Referans noktalarından elde edilen sinyal gücü ölçümleri merkezde toplanarak geometrik hesaplarla hedeflenen vericiye yönelik konum bilgisine ulaşılır.



Şekil 3.6. Üç ayrı konumdaki referans noktasından istifade ile konum değerlendirmesi

3.13.2. Kullanımı yaygın olan yön bulma teknikleri

Her ne kadar farklı şekilde tasnif edilseler de yaygın olarak kullanılan bazı yöntemler vardır. Her yöntemin de kendine has avantaj ve dezavantajları bulunmaktadır. Yöntem seçiminin; maksada, istenilen hassasiyete ve maddi kaynağa göre yapılması gerekmektedir.

RSSI

En basit ve en yüksek enerji verimliliğine sahip yöntemlerden biridir. Ancak, en büyük dezavantajı hassas pozisyonu tahmin zafiyetidir [43]. RSSI antenin sinyal üzerinden veri paketini aldığı anda ölçülen güç ile alakalıdır. RSSI, çeşitli konum belirleme algoritmalarında kullanılmaktadır. RSSI bilgisine alıcıya ulaşan veri paketinin IEEE 802.15.4 fiziksel katmanından ulaşılabilmektedir. RSSI değerini kullanarak ayrıca kanal modeli ve algoritma tasarımına bağlı olarak alıcı-verici arasındaki mesafeyi hesaplamak mümkündür [44].

Diğer tüm yöntemler gibi RSS de iki safhaya ihtiyaç duymaktadır: kalibrasyon ve konum belirleme. Kalibrasyon safhasında; bazı lokasyonlar için sinyal gücü bilgileri toplanır ve kanal parametreleri bu verilere göre tahmin edilir. Ölçümler ve kalibrasyon aşamasında bulunan kanal parametreleri kullanılarak hedef noktanın konumu belirlenir [45].

En yakın komşu (nearest neighbors - NN)

İlk olarak J.G. Skellam tarafından tanıtılmıştır. Gözlemlenen veri setti ile beklenen veri setti arasındaki mesafeler, sensörler ile okunan fiziksel parametrelerin türüne bağlı olarak muhtemel konumu belirlemek üzere kullanılır [37].

Varış zamanı (time of arrival - ToA)

Bu metot sinyalin alıcıya ulaştığı zamanlara arasındaki fark değil tam ulaşım zamanı tespitine dayanmaktadır. Sinyalin varış zamanı ve havada ışık hızında (300 000 km/sn) ilerlediği düşünülürse mesafe tahmini yapmak mümkündür. Ancak zaman tespitinin ve hesaplamanın hassas şekilde yapılması gerekmektedir [44].

2B bir koordinat veya istikamet belirlemek için en az üç ölçüm ünitesine ihtiyaç vardır. Ayrıca bu üç ünitedeki alıcı ve vericilerin tam senkron hale getirilmeleri gerekmektedir. Bu nedenle maliyeti yüksek zamanlama sistemine ihtiyaç duymaktadır. Uygun bir zamanlama sistemi; nanosaniye ile ölçülebilecek zaman ve dolayısı ile doğruluk oranı yüksek konumlama hizmeti sağlamaktadır [37].

Ulaşım zaman farkı (time difference of arrival-TDoA):

Sinyalin farklı antenlere farklı zamanlarda ulaşmasından hareketle sinyal istikameti hesaplanabilmektedir. Bu yöntem için en az 3 antene ihtiyaç bulunmaktadır. En iyi sonuç 3 antenin hedef vericinin etrafına yerleştirilmesi ile elde edilir. Diğer bir değişle bu yöntemde elde edilecek hassasiyet antenlerin yerine bağlıdır [42]. TDOA ilkesi, hedeflenen vericinin göreceli konumunu, vericiden çıkan sinyalin alıcılara ulaşma zaman farklarını kullanarak belirleme fikrinde yatmaktadır. Üç alıcı 2 TDOA sağlamaktadır. Böylece iki ölçümün kesişimi muhtemel konumu vermektedir. Bu da yine sistemlerin kesin zaman ayarına ihtiyaç duyan bir sistemdir. TDOA da TOA gibi sinyalin havada ilerleme süresinden istifade etmektedir. Dolayısı ile sinyalin yayılmasını etkileyen faktörler ölçümün etkinliğini düşürmektedir. Bu maksatla farklı sinyal işleme yöntemleri kullanılmaktadır [37].

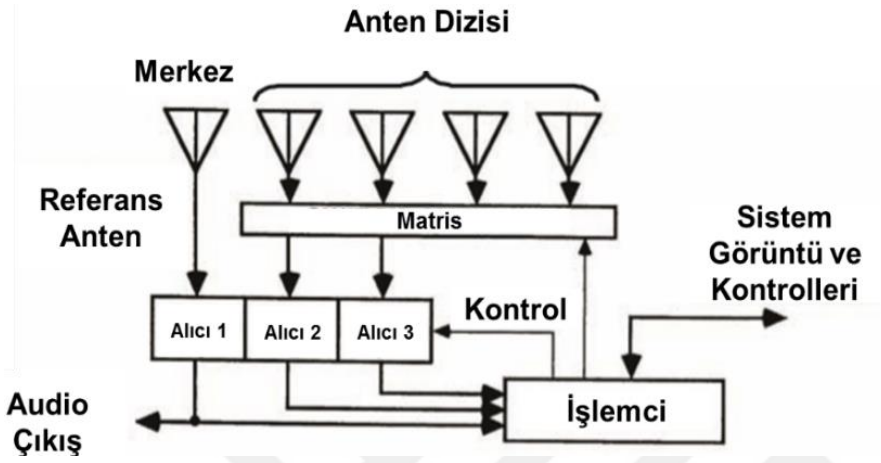
Ulaşım açısı (angle of arrival-AoA)

Vericiden alıcılara gelen sinyallerin oluşturduğu hatların kesişimi vasıtası ile hesap yapma yöntemini temel almıştır. Ulaşan sinyale yönelik bilgiler sinyalin faz farklarından tespit edilmektedir. Yönlendirilmiş anten veya antenler dizisi ile en az iki açı ölçülmelidir. Bu metot da diğerleri gibi gölgeleme (Shadowing) ve yansımalardan (Multipath Reflections) etkilenmektedir. Karmaşık ve pahalı sistemlere ihtiyaç duyması hasebiyle kendisi de pahalı bir yöntemdir [37].

Watson-watt yön bulma tekniği

Radar için yapılan ilk çalışmalardandır. Bu çok bilinen metot yön tespiti için Adcock antenlerini kullanmaktadır. Adcock antenleri her biri farklı bir kutup/yönde eşit aralıklarla yerleştirilmelidir. Antenler arasındaki mesafe faz farkına neden olmakta bu da istikametin belirlenmesinde kullanılmaktadır [42].

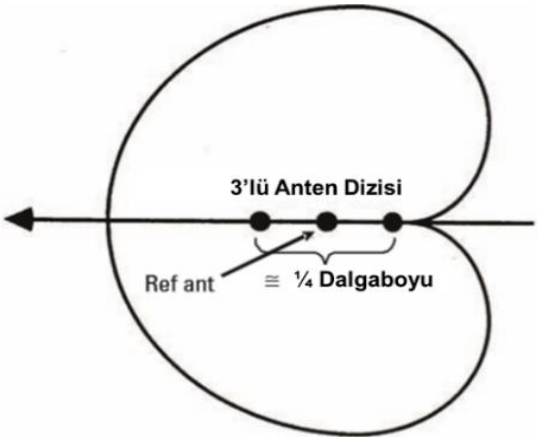
Watson-watt blok diyagramı Şekil 3.7'de görüldüğü gibi üç alıcı, en az 4 olmak üzere çift sayıda dairesel anten grubu ve referans anteninden oluşmaktadır. Dairenin çapı yaklaşık olarak dalga boyunun ¼'ü kadardır. Karşılık iki anten ve referans anteni alıcılara bağlanır. Dış iki anten ile referans antenin genlikleri karşılaştırılır.



Şekil 3.7. Watson-watt blok diyagramı [38]

Bu sinyallerin kombinasyonu üç anten etrafında Şekil 3.8'deki gibi kazanım paternini (geliş yönüne karşı kazanç) oluşturur. Dıştaki iki anten diğer karşılıklı iki anten ile değiştirilir ve bir kazanım paterni daha elde edilir. Birkaç kez bu işlem uygulandığında sinyal geliş istikameti hesaplanabilir.

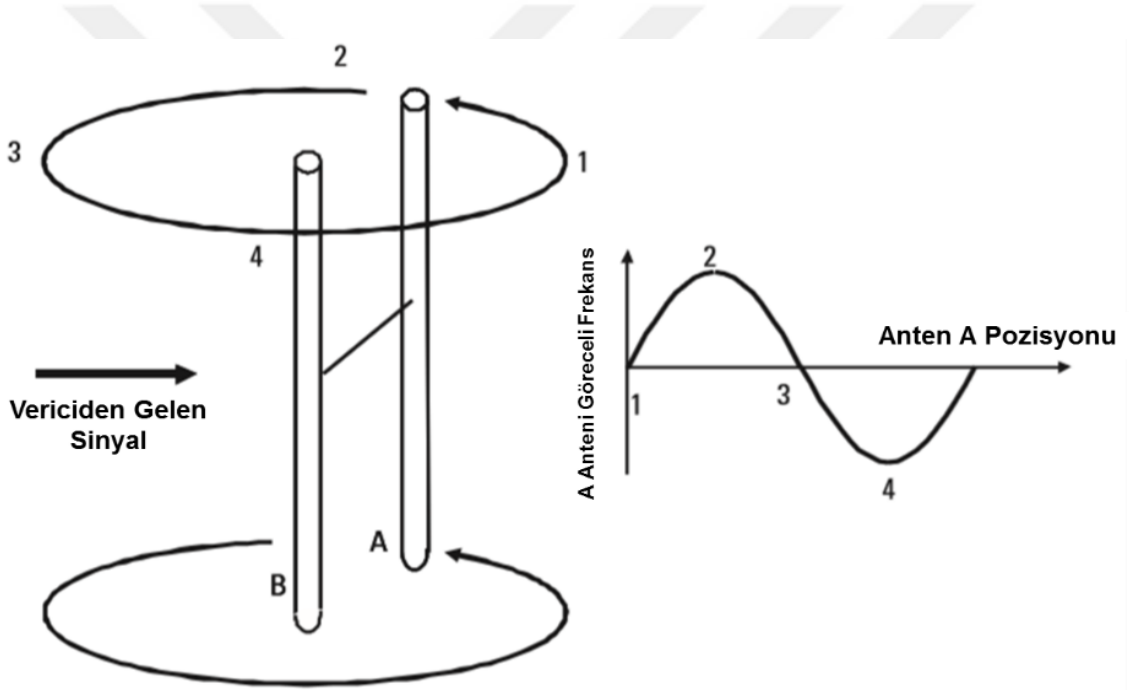
Watson-Watt her tür sinyal modülasyonuna karşı kullanılabilir ve kalibre edilmeden 2.5° dereceye kadar doğruluk sağlanabilir [38].



Şekil 3.8. Kazanım paternleri [38]

Doppler yön bulma tekniği

Bir anten diğerinin etrafında Şekil 3.9'daki Doppler konsepti çerçevesinde dönerse iki anten farklı frekansta sinyaller alırlar. Hareketli anten vericiye yaklaştıkça frekans Doppler etkisi ile artacak, uzaklaştıkça ise düşecektir. Bu değişim sinüs eğrisi şeklindedir ve sinyalin yönünün tespitinde kullanılabilir. Doppler yöntemi ticari maksatlı sıkça kullanılmakta, merkezdeki sabit antene ilave genel olarak üç antenden faydalanılmaktadır. Yönü 2.5° dereceye kadar doğrulukla tespit edebilmektedir. Ancak bu teknik, kendi modülasyonu, dış anten Doppler etkisinden ayırt edilemezse, frekans modülasyonlu sinyallere ilişkin zorluklara sahiptir.



Şekil 3.9. Doppler konsepti [38]

En küçük kareler metodu (method of least square-MLS)

Bu yöntem belirli bir örnek uzayda en iyi eşleşmeyi ya da kavise/eğime uyumu bulmak için kullanılmaktadır. Birbirine bağlı olarak değişen iki fiziksel büyüklük arasındaki matematiksel bağlantıyı, mümkün olduğunca gerçeğe uygun bir denklem olarak yazmak için kullanılan, standart bir regresyon yöntemidir. Yeni ve eski güç verileri arasındaki farkın kareler toplamını minimize etmeyi hedeflemektedir.

Maksimum olabilirlik metodu (maximum likelihood-ML):

Kavramsal olarak, sinyal ulaşım açısı her bir antende tespit edilen güç oranları kullanılarak belirlenebilir. Yine de ilave gürültüleri göz ardı ettiği için yeterli bir metot değildir. Yön tespitinde şu varsayımları kabul eder;

- Tüm kanallardaki sesler ortalama sıfır kabul edilir,
- Gürültü, olasılık yoğunluk fonksiyonlu Gauss dağılımına uygundur,
- Kanallardaki gürültüler birbirinden bağımsızdır.

Maksimum Olabilirlik Metodu varsayımlara dayanan olasılık fonksiyonlarını maksimize etmeye çalışır.

Çoklu sinyal tanımlama (multiple signal characterization-MUSIC):

Birden çok verici olduğunda sinyal istikametlerini ayrı tespit ederek konumlarını belirlemek maksadıyla geliştirilmiştir. Bu yöntemle belirlenebilecek verici sayısı kurulan tespit sistemindeki eleman (anten) sayısına bağlıdır. Maksimum Olabilirlik Metodu ile aynı varsayımları farklı şekilde kullanmaktadır. Her dizi elemanından alınan sinyallerin kovaryans matrisi özdeğerler ve özvektörlere ayrıştırılır. Teoriye göre, bazı özdeğerler eleman dizisi üzerine etki eden sinyallerle bazıları da gürültü ile ilişkilidir. Bu metot gelen sinyalin analizi üzerine kurulu olduğundan örneklem kümesi geniş olmalıdır. Gelen sinyal bileşenleri açısından kovaryans matrisinin ayrışma iyi bir başlangıç noktasıdır [42].

4. İNSANSIZ HAVA ARAÇLARINA KARŞI YAPILABİLECEK SALDIRI TÜRLERİ

Federal Havacılık İdaresi (Federal Aviation Administration - FAA) 2020 yılına kadar sadece ABD semalarında 30.000'den fazla insansız hava aracının (İHA) yer alacağını öngörmektedir [46]. Güvenlik ve özel yaşamın korunabilmesi için doğal olarak bu araçların yayılması dikkatli bir şekilde kontrol altında tutulmalıdır. Bu bağlamda, FAA'nın 2012 Şubat ayında kabul ettiği Modernizasyon ve Reform Yasası (Modernization and Reform Act) da 2015 sonuna kadar sivil İHA sistemlerinin ulusal havacılık sistemine güvenli bir şekilde bağlanmasını öngörmektedir [47]. Bahse konu karmaşık insansız sistemler saldırganlar tarafından ele geçirildiğinde/hacklendiğinde birer silaha dönüşme potansiyeline sahiptir. Bu sistemlere ilişkin bir başka soru işareti de uçuş esnasında topladıkları bilgileri (text, resim, video) depolama ve aktarmadaki veri yönetiminin güvenirliğine yöneliktir. İHA'ların teknoloji ve üretimine ilişkin endüstriyel bilgileri ele geçirmek için yapılan saldırılar, siber saldırılar, ağ istismarı ve kötü amaçlı yazılım saldırıların önemli bir kısmını kapsamaktadır.

İHA'ların çok ve çeşitli olması güvenliğe yönelik ciddi analizlerin yapılmasını gerektirmektedir. İHA sistemleri, her biri siber saldırıya maruz kalma potansiyeli yüksek ileri teknoloji parça ve alt sitemlerden oluşmaktadır. İHA'nın kontrolünün başka biri ya da bir grup tarafından ele geçirilerek İHA'yı asıl yönetenlere karışı kullanılması askeri güvenlik uzmanlarının kâbusu haline gelmiştir.

4.1. Otopilot Sistemleri

Günümüzde kullanılmakta olan birçok otopilot sistemi siber saldırılara karşı emniyetli olması düşüncesi ile tasarlanmamış ve üretilmemiştir ve bu nedenle siber saldırılara karşı korumasızdır. İHA sistemlerinin uçuşu çoğunlukla otopilot sistemlerine dayandığından muhtemel siber saldırılara karşı koyabilecek otopilot sistemleri tasarlamak büyük önem arz etmektedir. Zaten İHA'ların kullanımı askeri maksatları aşmış ve birçok alana yayılmıştır. Otopilot sistemleri genel olarak insanlı hava araçları için üretilmiş, insansız araçlarda kullanılmaya başlamış ve yapısında bir değişikliğe ihtiyaç duyulmamıştır. Bunun temel nedeni, insanlı araçlar için otopilot sistemi üretilirken siber güvenlik kavramının öne çıkan

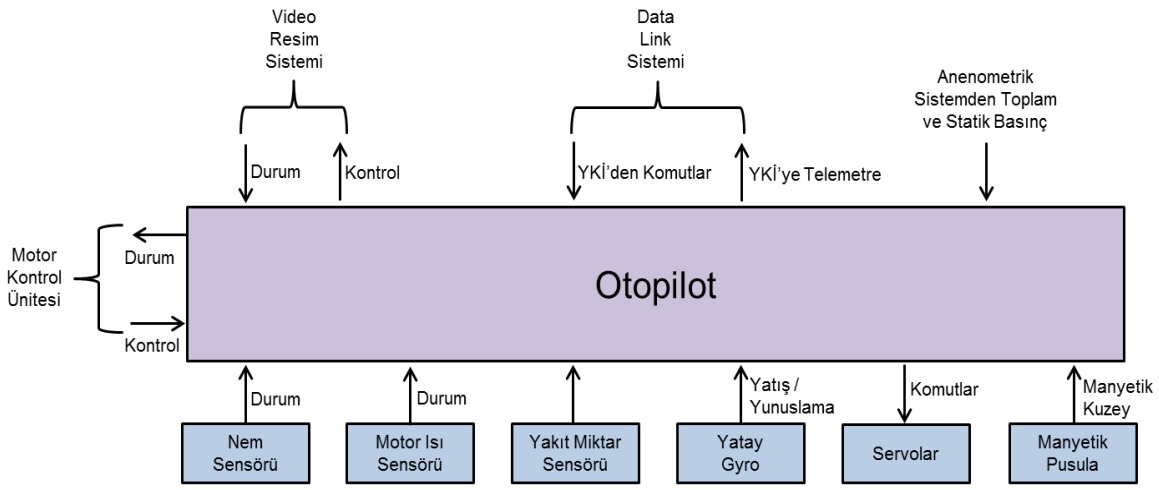
bir etken olmamasıdır. Bu durumun sonucu olarak da günümüz İHA sistemlerinin birçoğu kötü niyetli siber saldırılara karşı korumasız durumdadır.

4.1.1. İHA otopilot sisteminin temel unsurları

Genel bir İHA otopilot sisteminin içerisinde bulunan temel unsurlar aşağıdadır.

- Ana program ve işlemci: Sensörlerden gelen verilerin işlenmesi ve İHA'nın uçuş kontrolünden sorumludur.
- Manyetik pusula: Manyetik istikameti belirlemekte kullanılır.
- GPS: Küresel konumu belirlemede kullanılır.
- Altimetre: Hava kızı ölçümünde kullanılır.
- Veri linki: Yer istasyonu ile iletişimi sağlar.
- Elektrik sistemi: İHA'nın elektrik enerjisini sağlar.
- Gyro: İHA'nın yere göre pozisyonunu (yatış, dalış vb.) belirler.
- Servo: Hava aracının kontrolü için kullanılan elektrikli motorlardır.
- Manuel uçuş kontrol sistemi: Otopilotu devreden çıkararak kontrolü pilota bırakan sistemdir [48].

Örnek bir otopilot sistemi Şekil 4.1'de sunulmuştur.



Şekil 4.1. Örnek otopilot sistemi

4.1.2. Otopilot tehdit ve açıklık (zafiyet) tespiti

Otopilot üzerinden yapılan saldırılar incelendiğinde üç ana grupta toplandığı görülmektedir [48].

Donanım saldırıları

Saldırganın İHA otopilot sistemine doğrudan erişimi söz konusudur. Bu şekilde otopilot üzerinden akan verileri bozabileceği gibi sisteme ekleyeceği ilave donanım/yazılım ile de saldırının gerçekleştirilmesi mümkündür. Bu tarz saldırılar bakım, depolama, üretim ve dağıtım esnasında yapılabilir. Saldırgan otopilota doğrudan bağlanarak zarar verebileceği gibi yeniden programlayarak İHA'nın kontrolünü de ele geçirebilir.

Kablosuz saldırılar

Saldırı kablosuz veri linkleri üzerinden yapılabilir. Saldırganın kablosuz iletişim kanalına sızarak otopilota/hava aracı bilgisayarına müdahalesi ile gerçekleştirilir. Veriler üzerindeki şifrenin/kriptonun kırılması ile de İHA'nın tüm kontrolü ele geçirilebilir.

Sensör yanıltma

Saldırganın doğrudan İHA üzerindeki sensör/alıcılara yanıltma sinyali göndermesi ile gerçekleştirilir. Yanıltma için GPS, radar, IR vb. sensörler tercih edilebilir. İHA uçuşları esas olarak GPS verilerine dayanmaktadır. Bu nedenle yanıltmalar ciddi olaylarla sonuçlanabilir. Sensör yanıltmaları iki gruba ayrılabilir:

Kontrol sistem güvenliği

Donanım/CPU'nun programlandığı şekilde çalışmasını önlemek. Sistemin sıfırlanması (reset), kötü niyetli yazılım yüklenmesi, donanım değişiklikleri ve sisteme ilavelerle arabelleğin aşırı yüklenmesi (buffer overflow) bu yönteme güzel bir örnektir.

Uygulama mantık güvenliği

Sensörleri manipüle ederek kontrol sistemine giden verileri değiştiren saldırı türüdür. Bu durumda tüm uçuş sistemleri programlandığı şekilde çalışmasına rağmen işledikleri veriler doğru olmayan verilerdir. Bazı örnekleri; veri manipülasyonu, sistem durum bilgisinin manipülasyonu, seyrüsefer bilgilerinin ve komuta kontrol verilerinin manipülasyonudur.

4.2. Yaygın Olarak Kullanılan Saldırı Yöntemleri

4.2.1. GPS spoofing

Bahse konu saldırılardan en yaygını ve etkili olanı GPS'in yanıltılması (GPS Spoofing) saldırısıdır. Düşük bant genişliği, zayıf sinyal gücü ve zayıf yetkilendirme mekanizması ile GPS sinyali kolayca karıştırılabilir, geciktirilebilir veya az bir enerji ile geniş bir alanda taklit edilebilir. Bu taklit sinyali GPS vasıtası ile alan sistem hata olduğunun farkına varmaksızın kendi konumu hakkında yanlış yönlendirilmiş olur. USRP (Universal Software Radio Peripheral) vb. programlanabilir sinyal platformlarının gelişimi ile birlikte sahte GPS sinyali üreten simülatör geliştirmek oldukça kolaylaşmıştır.

GPS spoofing saldırısının ilk adımı yayımlanan sinyalin GPS'in hâlihazırda almakta olduğu sinyal ile senkronize edilmesidir. Bunun ardından sahte sinyalin orijinal sinyalin yerini alması gelir. Sonuç olarak GPS gerçek sinyaller yerine tamamen sahte sinyaller ile konum bilgisi üretmeye devam eder. GPS'in ele geçirilmesi ile birlikte saldırgan istediği sahte konumları İHA'ya göndermiş olur [49].

<u>GPS spoofing yöntemleri</u>

GPS spoofing yöntemleri genel olarak üç gruba ayrılmıştır [46].

GPS sinyal simülatörü

Sahte sinyalin gerçek sinyal ile senkronizasyonuna ihtiyaç duymadan çalışan bir sistemdir. Aşırı gürültülü çalışmasına rağmen ticari GPS'lere karşı oldukça etkilidir. Ancak bu yöntemle üretilen sahte sinyal kolayca tespit edilebilmektedir.

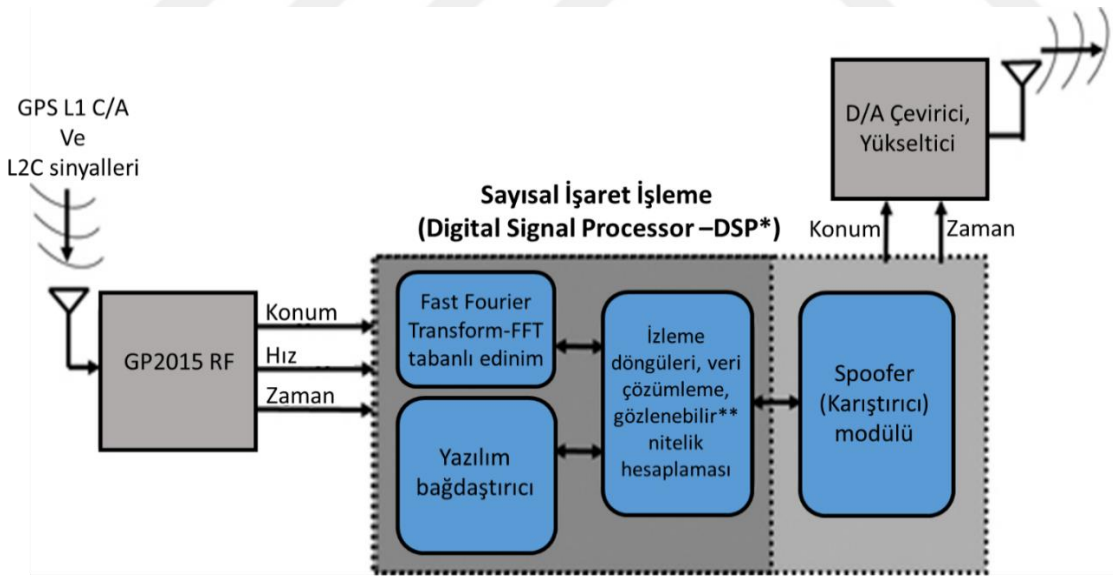
Alıcıya (receiver) dayalı yanıltıcılar

GPS alıcısı, yanıltıcının göndermeci (transmitter) ile birlikte çalışır. Bu teknikte sahte sinyalin gerçek sinyal ile senkronizasyonuna ihtiyaç vardır. Ancak ondan sonra GPS konum, zaman açısından yanıltılabilir. Bu teknik tespiti zor ama hedef GPS ile yüksek korelasyon gerektirdiği için karmaşık olan bir yöntemdir.

Alıcıya dayalı gelişmiş yanıltıcılar

Bu yöntemde, sinyalin mükemmel olarak senkronize edilebilmesi için hedef GPS alıcı antenin koordinatı tam olarak bilinmelidir. Birçok anten kullanılarak, aldatmaya karşı kullanılabilecek yöntemlerin aşılabilmesi bu yöntemin avantajlı yönüdür. Bu avantajına rağmen en karışık, uygulaması en zor yöntemdir. İHA'daki GPS anteninin yerinin ve geometrisinin devamlı değişmesi nedeniyle imkânsız olarak değerlendirilmektedir.

Örnek bir GPS aldatıcının (spoofer) şematik gösterimi Şekil 4.2'de sunulmuştur.



Şekil 4.2. Örnek GPS spoofer [50]

Bahse konu aldatıcı bugüne kadar GPS verilerini ve sinyalini tam olarak senkronize ettiği rapor edilen tek aldatıcıdır. Böyle bir aldatıcı ile kullanıcı taraf farkına dahi varamadan ve hiç iz bırakmadan etkili bir aldatma işlemi gerçekleştirilebilir [47].

Aldatıcı öncelikle İHA GPS sinyalini tespit ederek GPS L1 C/A ve L2C sinyallerini izler. Anteni ile elde ettiği sinyalinin sahtesini oluşturur. Geri besleme sinyali aldatıcı tarafından izlenir ve dijital sahte sinyal üretimi ile analog sahte sinyal çıkışı arasındaki gecikme kalibre edilir. Bu husus, alıcı çalıştığında gecikme belirsiz olduğu için gereklidir, ancak sonrasında gecikme sabit kalır. Kalibrasyon tamamlandıktan ve seyrü sefer verilerini hazırlamak için yeterli zaman geçtikten sonra saldırgan GPS aldatma faaliyeti için hazırdır. Öncelikle senkronize edilmiş ama zayıf bir sinyal yayımlar. Ardından aldatıcı sinyal seviyesi asıl GPS sinyal seviyesini geçene kadar yavaşça artırılır. Bu noktadan itibaren hedef alıcının kontrolü ele geçirilebilir. Ancak şu iki hususdan biri meydana geldiğinde aldatmanın gerçekleştiği kabul edilebilir:

- Taklit edilen her sinyal asıl sinyale oranla 2 μs artırıldığında veya
- Taklit edilen her sinyal asıl sinyalden en azından 10 dB daha güçlü olduğunda [46].

Bu aldatıcı birçok kez teste tabi tutulmuş ve her seferinde başarılı olduğu görülmüştür.

Fark edilme durumuna göre GPS spoofing

Tüm GPS spoofing teknikleri saldırganın saldırısını gizlemesi (covert capture) veya gizlememesi (overt capture) durumuna göre ikiye ayrılmaktadır. Tahmin edilebileceği gibi covert capture metodu gerçekleştirmesi zor ve diğer tekniğe göre erişimi sınırlı olanıdır [51].

Overt Capture

Saldırgan faaliyetini gizleme kaygısı taşımamaktadır. Bu nedenle sinyali başlangıçta taklit etmek yerine önce sinyali karıştırarak İHA'nın kontrol dışı kalmasını sağlayıp ardından ürettiği sinyalle İHA'nın kontrolünü ele geçirebilir.

Covert Capture

Bu tarz saldırıda hedef GPS'in saldırı tespit sistemi ile donatıldığı varsayılarak sistemin tetiklenmesinden kaçınılır. Bu teknikler üzerinde halen çalışılmaktadır. Bazılarının uygulanması çok zor bazılarınınki de çok pahalıdır. Eğer saldırgan aşağıdakileri sağlayabilirse covert capture sınıfında bir saldırı düzenlediği kabul edilir:

- Overt capture saldırının tüm gereklerini sağlamış olmak,
- Aşağıda açıklanan tespit tekniklerinden kaçınmış olmak;
  - GPS alıcısında karıştırma-gürültü (Jamming-to-noise J/N) tespiti: Belirli bir bant genişliğinde alınan sinyal gücü normal seyrine oranla önemli derecede artarsa alarm tetiklenir. Piyasada çok az miktarda J/N tespit sistemi içeren GPS bulunmaktadır.
  - GPS alıcısında frekansa erişim (frequency unlock) tespiti: Saldırı olmadığı durumda çok nadir karşılaşılan bir olay olduğundan ve saldırı için de gerekli bir husus olduğundan etkili bir saldırı tespit yöntemidir.
  - Navigasyon sisteminin durum tahmincisi (state estimator) içinde yenilik testi: Kolayca uygulanabilecek bir yöntemdir. GPS'inkiler dışındaki sensörlerin durum tahmincisine gönderdiği veriler ile karşılaştırma yaparak bir tespitte bulunulur. Tespitin hassasiyeti diğer sensör verilerinin güvenilirliğine bağlıdır.

GPS spoofing etkileri

İnsanların böyle bir saldırıyı yapması mümkündür ve bunu yapmak için birçok farklı sebepleri olabilir. Bu da alçak/orta irtifada diğer hava araçları ya da binalarla İHA'ların çarpışmalarını sağlayacak ciddi sonuçlar doğurabilir. Her şeye rağmen (Bkz) Şekil 4.2'deki gibi bir aldatıcı yapmak kolay da değildir, ortalama bir saldırganın imkân kabiliyetleri dâhilinde de değildir. Ancak yapılan ARGE çalışmaları neticesinde elde edilen teknolojik gelişmeler bu hususu da gün geçtikçe kolaylaştırmaktadır.

Referans olması açısından; dünya üzerinde, üniversitelerden 100'den fazla araştırmacının bir yılını adadığı takdirde bu tarz bir aldatıcı geliştirebileceğini söylemek mümkündür [47]. Olayın daha önemli tarafı ise bir İHA'yı aldatmak için yukarıda anlatılan çapta bir aldatıcı yapılmasına ihtiyaç olmadığıdır. Düşük maliyetli ve satışa hazır olan, GPS sinyalini simüle edebilen cihazlar da İHA'yı ele geçirmek için yeterli olmasa da GPS sinyalini karıştırmak ve/veya bastırmak için yeterli olabilecek durumdalardır.

Araştırmacılar, birden çok GPS alıcı anteni kullanılarak belirlenen koordinatları karşılaştırma sonucunda yanlış olan sinyalin tespit edilebileceğini ileri sürmektedirler. Örneğin, iki adet alıcı anteni kullanılarak bir saldırı yapıldığı tespit edilebilir: normal olarak iki antenden elde edilen koordinatlar farklı olması gerekirken böyle bir saldırı durumunda iki koordinat da ufak zaman fasıla haricinde aynı olur [52].

GPS spoofing saldırısına karşı alınabilecek tedbirler

Bu maksatla kullanılabilecek en gelişmiş teknikler şunlardır [53]:

Genlik ayrımı (amplitude discrimination)

Genlikdeki ve sinyal/gürültü oranındaki değişimler muhtemel saldırının tespiti için kullanılabilir. Normalden daha güçlü bir GPS sinyali gelirse bu sinyal reddedilebilir.

Ulaşım zamanı ayrımı (time-of-arrival discrimination)

Senkronize edilmeyen sinyaller ulaşım zamanlarında farklılıklar meydana getirir ve zaman kaymasına (clock-offset) neden olur. Kısa zamanda içerisinde büyük bir clock-offset saldırının en iyi belirtisidir.

Navigasyon atalet ölçüm birimi tutarlılığı kontrolü (consistency of navigation IMU cross-check)

IMU ivmeölçer ve gyrolar yardımıyla hareketleri tespit ederler. Başlangıç pozisyonu biliniyorsa belirli bir zaman sonraki konum da tespit edilebilir. Yapılan hesap sonucu elde edilen veri ile GPS verileri karşılaştırılarak saldırı mevcudiyeti tespit edilebilir. Doğal olarak bu yeteneklere sahip bir alıcının maliyeti de yüksek olacaktır.

Polarizasyon ayrımı (polarization discrimination)

Alıcılar farklı polarizasyona sahip sinyalleri tespit edebilirler. Yeteneksiz veya acemi bir saldırganın yaptığı saldırı tespitinde bu yöntem işe yarayabilmektedir.

Ulaşım açısı ayrımı (angle-of-arrival discrimination)

GPS sinyalleri farklı göndermeçlerden gönderildiğinde alıcıya ulaşma açıları da birbirinden farklı olmaktadır. Ancak genelde saldırganlar da tek anten kullanmaktadırlar. Bu durumda saldırı ancak sinyalin geliş açısı ile normalde gelmesi beklenilen açı kıyaslanarak tespit edilebilir.

Artakalan sinyal savunması (vestigial signal defense)

Saldırgan eğer GPS'e doğrudan fiziksel erişimi yoksa asıl Navigasyon sinyalini ortadan kaldıramayacaktır. Artakalan bu asıl sinyaller tespit edilerek de saldırının varlığı belirlenebilir.

Konumsal zıplamalar (jumps in space)

Basit bir tespit yöntemi de konum verilerindeki değişikliklerin izlenilmesidir. Bir İHA'nın hızı ve hareket yönü göz önünde bulundurulduğunda normal olmayan yer değişiklikleri de saldırının belirtisi olabilir.

4.2.2. GPS sinyalinin karıştırılması (signal jamming)

Bu yöntemi kullanarak İHA'nın uydulardan gelen GPS sinyalini alması önlenebilir. Bu durumda İHA konumunu, irtifasını ve uçuş istikametini hesaplayamadığı için rotasını da kaybedecektir. Günümüzde düşük fiyatlı temin edilebilecek GPS karıştırıcıların (jammer) sayısındaki artış nedeniyle "GPS sinyal karıştırma"nın yakın gelecekte önemli bir sorun olacağı öngörülmekte bu nedenle de İHA'lar için GPS'e dayalı olmayan seyrü sefer yöntemleri geliştirilmeye çalışılmaktadır. Bir İHA'nın GPS sinyallerinin karıştırılması durumunda İHA pilotu tüm kontrolünü kaybedecek, İHA ya düşecek, ya acil durum (emergency) uygulamaları ile kurtarılabilecek ya da yakıtı tükenene kadar uçacaktır [46].

4.2.3. Siber saldırı kötü amaçlı yazılımları (malware)

İHA'nın bileşenlerinde yazılım da bulunduğundan siber saldırılara uğraması her zaman olasıdır. Kötü amaçlı yazılım tehdidi ciddi bir sorundur. Son dönemlerde gerçekleşen siber saldırılar yüksek gizlilikteki çevreyi de vurmuştur. Bahse konu kötü amaçlı yazılımlar zero-day açığını kullanarak sistemin güvenlik kontrollerini aşmış ve gelişmiş bir araca zarar vermiştir. Bu saldırı benzeri olaylar İHA'lar için de potansiyel tehdit oluşturmaktadır. Bir diğer önemli husus da İHA'ların üretimi esnasında farklı firmalardan temin edilen çok miktar ve çeşitlilikteki sistem parçalarının oluşturduğu zaaftır. Bir saldırganın bu parçaların farklı açıklıklarını tespit ederek hava aracının tamamını etkileyebilecek bir saldırı yapması muhtemeldir [46].

4.2.4. Siber casusluk (cyber-espionage)

Göreceli olarak önemli tehditlerden biridir. İHA'lar öncelikli hedefleri arasındadır. Saldırgan İHA'dan önemli bilgileri çalabilmek için "oltalama saldırısı (spear-phishing)" düzenler. Bu maksatla e-posta göndererek ve/veya zararlı yazılım içeren bir web sitesini ziyaret edildiğinde zararlı yazılımın kullanıcı bilgisayarına bulaşması (drive-by downloads) neticesinde "Truva atı arkakapıları (Trojan backdoor)" yüklenir ve PDF veya DOC gibi belgelerin açıkları kullanılır [46].

4.2.5. Küresel navigasyon uydu sistemi (global navigation satellite system-GNSS) spoofing

GNSS aldatmaya (spoofing) karşı birkaç etkili yöntem bulunmaktadır. Bunlar aşağıdaki şekilde gruplandırılabilir:

- Alıcı-otonom sinyal işleme odaklı teknikler: Herhangi bir antene ya da anten donanımına ihtiyaç duymazlar.
- Alıcı-otonom anten odaklı teknikler: Antene ya da anten donanımına ihtiyaç duyarlar.
- Kriptografik teknikler: Mevcut veya gelecekteki sivil GNSS sinyalleri üzerinde kanıtlanabilir modülasyonlar hariç öngörülemeyeni de kapsaması için sinyal özellik modifikasyonuna ihtiyaç duyar.
- Mevcut kriptolu askeri sinyalleri sivil GPS alıcıları için kimlik doğrulama maksadıyla kullanan teknikler.

Maalesef bu tekniklerin olgunlaşması ve yaygınlaşması için biraz daha zamana ihtiyaç bulunmaktadır. Hâlihazırda GNSS aldatılmasına karşı rafta hazır ürün bulunmamaktadır [51].

4.2.6. Video görüntüsünün ele geçirilmesi (video capturing)

Herhangi bir şifreleme ya da kriptolama tekniği uygulanmamış görüntü hava aracından yer kontrol istasyonuna gönderildiğinde aynı frekanstaki ve görüş hattı üzerinde bulunan başka bir alıcı vasıtası ile görüntünün ele geçirilerek kaydedilmesi, işlenmesi ve dağıtılması

mümkündür. “SkyGrabber” adında bir yazılımın bu maksatla kullanıldığı bilinen bir gerçektir. Bu yazılım uydu antenleri vasıtası ile havadaki resim ve video sinyallerini yakalayabilmektedir. Bu yöntemle resim ve videonun yanı sıra hava aracı uçuş bilgilerinin (telemetre) de ele geçirilmesi mümkündür. Tek ihtiyaç havadaki sinyali tespit etmek için kullanılabilecek C-Bant veya Ku-Band anteni ile alıcısıdır [54].

4.3. İHA’nın Tespit ve Takibi

Bu maksatla kullanılabilecek dört yöntem bulunmaktadır. Klasik gözetlemede, uçaktan gelen radar ve işaretçi (beacon) sinyallerinin tespitine dayanmaktadır. Gözle tespit de klasik bir yöntem olarak kabul edilmektedir. Akustik algılama yönteminde İHA’ların elektrikli/benzinli motorlarının kendilerine has akustik işaretleri izlenerek yer ve iz tespiti yapılabilir. Radyo salınım algılamada, hava araçlarının yer kontrol istasyonuna kablosuz veri linki vasıtasıyla gönderdiği veriler yönlendirilmiş bir antenle tespit ve takip edilebilir. Elektro-optik (EO) algılama yönteminde ise hava aracı üzerindeki kameraların ve EO sensörlerin görülebilir ışığa ve kızılötesi ışımaya karşı hassasiyetinden istifade ile İHA’ların yeri tespit ve takip edilebilir [55].

4.4. Örnek Tespit ve Saldırı Olayları

6 Ekim 2012 tarihinde İran’a ait bir insansız helikopter İsrail üzerinde keşif/gözetleme yapmak maksadıyla Lübnan’dan havalanmış, İsrail tarafından tespit edilmiş ve üzerinde patlayıcı olabileceği değerlendirilen helikopter bir orman üzerinde İsrail yapımı Piton havadan havaya füzeleri bulunan F-16 savaş uçakları tarafından vurularak düşürülmüştür [56].

Todd E. Humphreys başkanlığında bir grup Teksas Üniversitesi öğrencisi üniversiteye ait mutfak masası büyüklüğünde bir İHA’nın GPS sinyallerini taklit ederek kontrolünü ele geçirdiklerini açıklamışlar ve ayrıca bir gösterimini de yapmışlardır. Grup lideri ve mühendislik bölümü öğrencisi Daniel Shepard tarafından, üretilen cihazın 1.000 dolara mal olduğu ve dört yıllık çalışmanın ürünü olduğu ifade edilmiştir [57].

Almanya'ya ait bir Heron 8 Kasım 2013 tarihinde düşmüş, olayın ardından İsrail tarafından yapılan açıklamada olayın basit bir kaza olmadığı, aksine büyük olasılıkla İran tarafından gerçekleştirilen bir GPS hacklemesi sonucu meydana geldiği iddia edilmiştir [58].

ABD'ye ait RQ-170 ve MQ-1 Predator tipi İHA'ların mobil yer kontrol istasyonlarında bulunan bilgisayarlara virüs bulaştığı; bu olayın İHA'yı hackleyerek kontrolünü ele geçirmek veya düşürmek için gerçekleştirilmiş olabileceği iddia edilmiştir [59].

ABD'ye ait bir keşif İHA'sının Ukrayna'nın Kırım Bölgesi üzerinde görevde iken Rusya Federasyonu tarafından hacklendiği yakın zamanda yayımlanan bir rapora yansımıştır [60].

Amerikalı bir İHA pilotu; General Atomics'e ait bir MQ-1 Predatorün kontrolünün ele geçirildiği ve üzerindeki silahlar ile yerde bulunan olaydan habersiz birliğin üzerine atış yapıldığını hayret ve korku içerisinde nasıl izlemek zorunda kaldığını açıklamıştır. Olayın sorumlusunun İngiliz hacker Derek Yates olduğu belirtilmiştir [61].

Aralık 2011 ayında dünya üzerinde bilinen en önemli İHA ele geçirme olayı gerçekleşmiştir. ABD CIA'ye ait bir RQ-170 Sentinel model İHA, İran tarafından kontrolünün ele geçirilmesinin ardından çok az bir hasarla yine İran tarafından yere indirilmiştir. İran tarafından ele geçirilen İHA Resim 4.1'de sunulmuştur. İranlı bir mühendis olayın ardından yaptığı açıklamada; İHA'nın sinyalinin bastırılarak tamamen GPS'e dayalı otopilot tarafından otonom uçuşa geçirildiğini ve bunun ardından sahte GPS sinyalleri vasıtasıyla İHA'nın indirildiğini ifade etmiştir [47].

Resim 4.1. İran tarafından ele geçirilen İHA [62]

2013 yılı içerisinde Afganistan ve Pakistan'da ABD CIA'ye ait İHA'ların Taliban tarafından ele geçirilmeye çalışıldığı, teröristlerin bu olayı gerçekleştirmek için yeterli teknik eğitimi edinmiş olabilecekleri iddia edilmiştir [63].

4.5. Siber Saldırılara Karşı Neler Yapılabilir?

İHA'larda siber savunma kapsamında alınabilecek tedbirlere ilişkin üç önemli fikir bulunmaktadır:

- Her denetleyicide bulunacak bir ana kesme anahtarı ile tespit edilecek şüpheli durumlarda İHA'nın tüm elektrik gücü ya da söz konusu İHA'nın denetleyici ile uyumlu tamamen şifreli kontrol sinyali kesilebilir.
- İHA sistemine ait işletim sistemi küçük hafıza kartlarına yüklenerek görev dışında kartların İHA pilotları tarafından sökülmesi sağlanabilir.
- İHA kullanıcılarına yönelik sertifika eğitimleri verilirken müfredata siber güvenlik konuları da eklenebilir.

Bunların dışında geleneksel yöntemler olan güvenlik duvarı (firewall) ve anti-virüs programları da kullanılabilir [64].

4.5.1. Tamamen yeni bir programlama dili oluşturulması

ABD Savunma Bakanlığı İleri Araştırma Projeleri Ajansı (Defense Advanced Research Projects Agency-DARPA) halen "hacklenemez" olacağını belirttikleri yeni bir programlama dili üzerinde çalışmaktadır. 2017 yılının sonuna kadar Boeing H-6U üzerinde uygulanması beklenilmektedir.

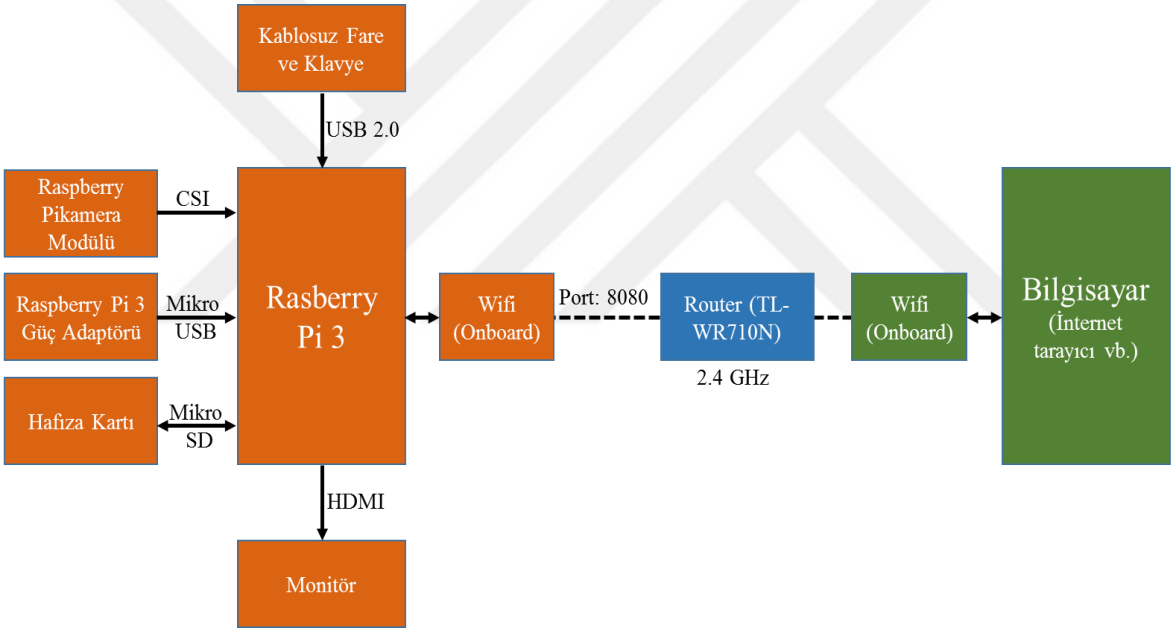
Hâlihazırda İHA'lar için programlar yazılırken C veya C++ dilleri kullanılmaktadır. Ve bu iki programlama dilinin de açıklıkları olduğu bilinmektedir. Buna rağmen ABD'li bir İHA firması bahse konu açıklıkların giderildiği C++ tabanlı bir yazılım geliştirdiklerini de ifade etmiştir.

Boeing firması tarafından İHA yazılımının 100.000 satırlık koduna tekabül eden % 70'lik bölümü değiştirilmiş ve yeni yazılımın uçuş esnasında hackleme çalışmasının 2015 yılı sonuna kadar deneneceği açıklanmıştır [65].

5. İNSANSIZ HAVA ARAÇLARI İÇİN GELİŞTİRİLİLEN GÜVENLİ GÖRÜNTÜ AKTARIM METODU

5.1. Geliştirme Ortamı

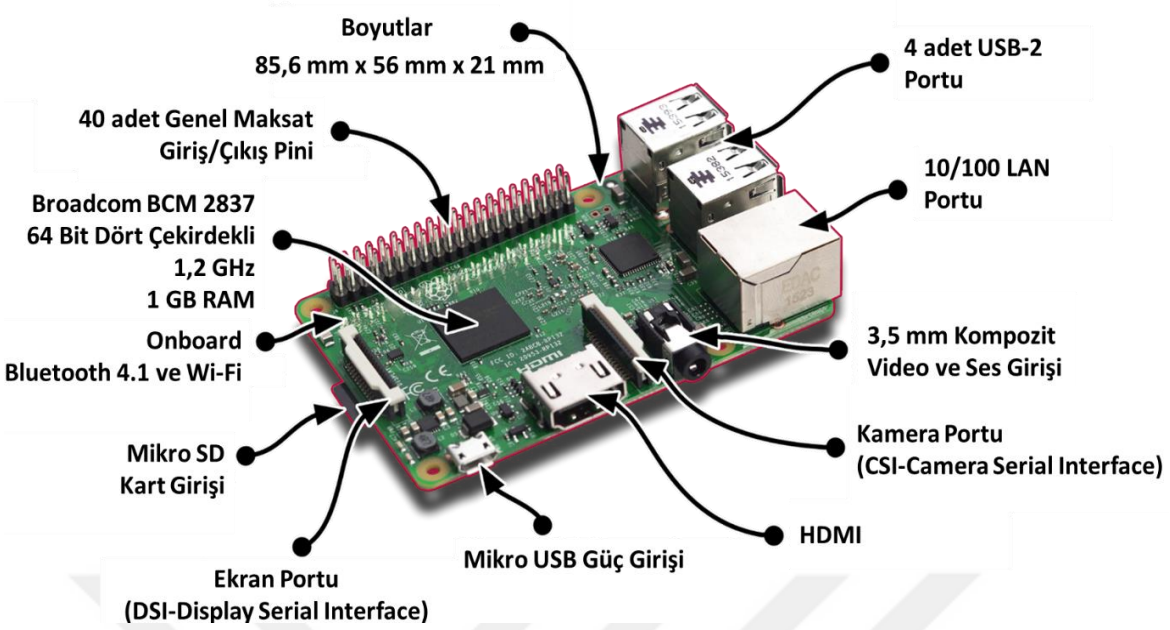
Güvenli veri linkine yönelik çalışma yapılabilmesi için öncelikle üzerinde yazılımsal geliştirme ve denemeler ile uygulamaların yapılabileceği, İHA, üzerindeki kamera ve aşağı/yukarı veri linkini de temsil edebilecek bir ortam, Şekil 5.1'de sunulan sistem blok diyagramına uygun oluşturulmuştur. Bunun için, kredi kartı büyüklüğünde tasarlanmış bir bilgisayar olan Raspberry Pi 3 ve ilave donanımı tercih edilmiştir.



Şekil 5.1. Sistem blok diyagramı

5.1.1. Raspberry Pi 3

Raspberry Pi İngiltere'de Raspberry Pi Vakfı tarafından okullarda bilgisayarı öğretmek maksadıyla tasarlanmış tek kartlı bilgisayardır. Özellikleri Resim 5.1'de görülmektedir. Çalışmamız için özellikle Wİ-Fi, HDMI giriş, Mikro SD kart girişi, güç girişi, Camera Serial Interface (CSI) girişi ve USB portu kullanılmıştır. Kartın Linux işletim sistemi ile kullanılmasına karşın bazı uygulamalarda Windows kullanımına da rastlanılabilmektedir.



Resim 5.1. Raspberry Pi 3 özellikleri

5.1.2 Raspberry Pikamera modülü (Picamera, Rev. 1.3)

Resim 5.2'de sunulan Raspberry Pikamera Modülü (versiyon 1.3), 5 megapiksel (2592×1944) çözünürlükte sabit odak noktalı bir kameraya sahiptir. Üzerinde Sony tarafından üretilen IMX 219 PQ CMOS görüntü algılayıcı sensör bulunmaktadır. Raspberry Pi ile CSI konektörü üzerinden bağlantı yapılmaktadır. 1080p çözünürlükte 30 fps, 720p çözünürlükte 60 fps veya 640x480p çözünürlükte 60/90 video aktarabilmektedir.

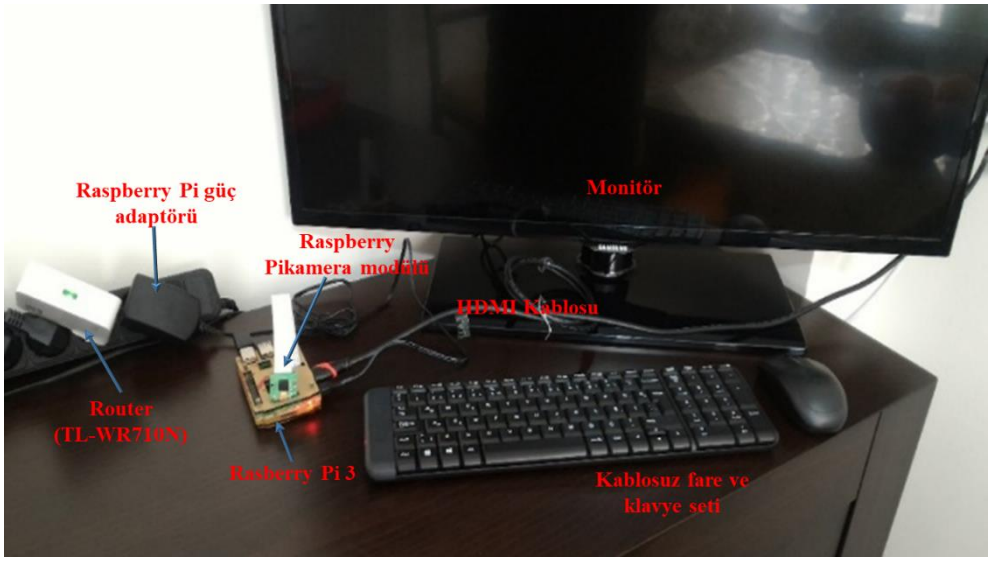
Resim 5.2. Raspberry Pikamera modülü

5.1.3. Router (TL-WR710N)

Hava aracı ile yer veri terminali arasında bulunan iki taraflı (aşağı/yukarı) veri linkini temsil etmek üzere bilgisayar ve Raspberry Pi 3 arasında gerekli bağlantıyı sağlayabilmek için yerel alan ağını (LAN-Local Area Network) oluşturmak maksadıyla kullanılmıştır. Çalışmada kullanılan Tp-Link marka ve TL-WR710N model cihaz, 2.4 GHz frekansı ile IEEE 802.11n, IEEE 802.11g ve IEEE 802.11b kablosuz standartlarını desteklemektedir.

5.1.4. Raspberry Pi 3 çevre birimleri

Raspberry Pi 3 işlemcisi, 13 W çıkış gücünde, 2,5 A ve 5,1 V çıkış gerilim veren mikro USB girişli bir adaptörden beslenmiştir. İşlemcinin kendi hafızası bulunmadığından işletim sistemi harici 16 GB kapasiteli SD karta yüklenmiştir. Ayrıca Rasberry Pi'nin çıkış birimine HDMI kablosu kullanılarak HDMI girişine sahip bir monitör bağlanmıştır. Raspberry Pi'ye giriş birimi olarak da USB Fare/Klavye Seti kullanılmıştır. Şekil 5.1'de sunulan görüntü aktarım sistemi blok diyagramı çerçevesinde yukarda özellikleri sunulan donanımdan teşkil edilen görüntü aktarma temsili ortamı Resim 5.3'de görülmektedir.



Resim 5.3. Görüntü aktarma temsili ortamı

Temsili ortamda yapılan geliştirme ve denemeler neticesinde, Raspberry Pi 3, pikamera ve güç kaynağından oluşan güvenli görüntü aktarım sisteminin quadkoptere entegre edilmiş şekli Resim 5.4'de sunulmuştur.

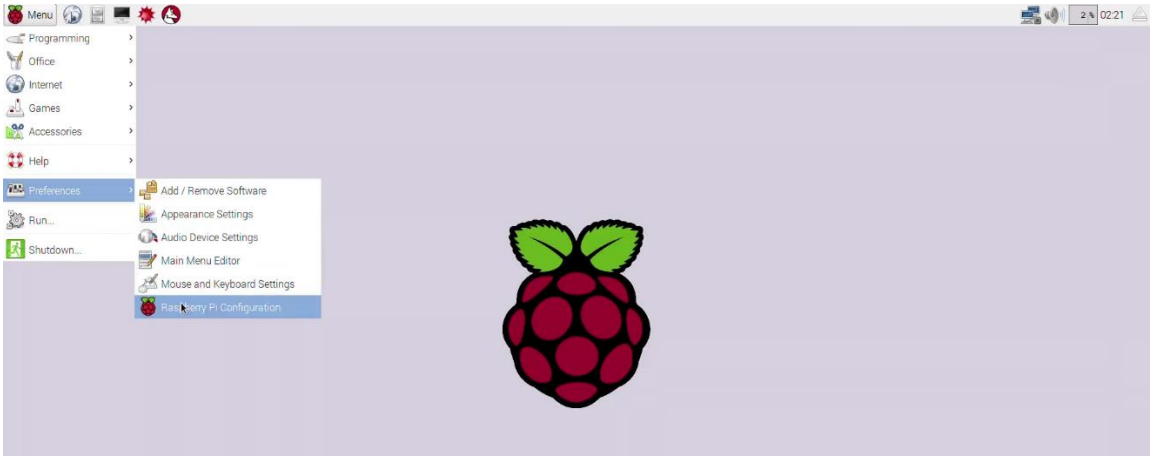
a) b)

Resim 5.4. Güvenli görüntü aktarım sisteminin quadkoptere entegre edilmiş şekli

a) Küçük quadkopter (30*30) b) Büyük quadkopter (50*50)

5.2. İşletim Sistemi

Raspberry Pi 3'e başlangıç seviyesi kullanıcılar için yeni geliştirilmiş olan NOOBS işletim sistemi kurulmuştur. İşletim sistemi, eğitim için ihtiyaç duyulan çeşitli yazılımları (LibreOffice, Python, Scratch, Sonic Pi, Java, Mathematica, vb.) içermektedir. Rapberry Pi işlemcisine yüklenmiş NOOBS işletim sistemi kullanıcı arayüzü Resim 5.5'de sunulmuştur.



Resim 5.5. NOOBS işletim sistemi kullanıcı arayüzü

Kablolu/Kablosuz internet bağlantısı yapıldıktan sonra açılan linux terminal üzerinden aşağıdaki komutlarla güncelleme işlemi yapılmıştır.

- sudo rpi-update => firmware güncellemeleri için,
- sudo apt-get update & upgrade => işletim sistemi güncelleştirmeleri için.

Linux terminal üzerinden verilecek “sudo raspi-config” komutu ile ya da menüden seçilecek “Raspberry Pi Configuration” ile açılan pencerede kamera aktif hale getirilmiştir.

5.3. Çalışmada Kullanılan Programlama Dili: Go

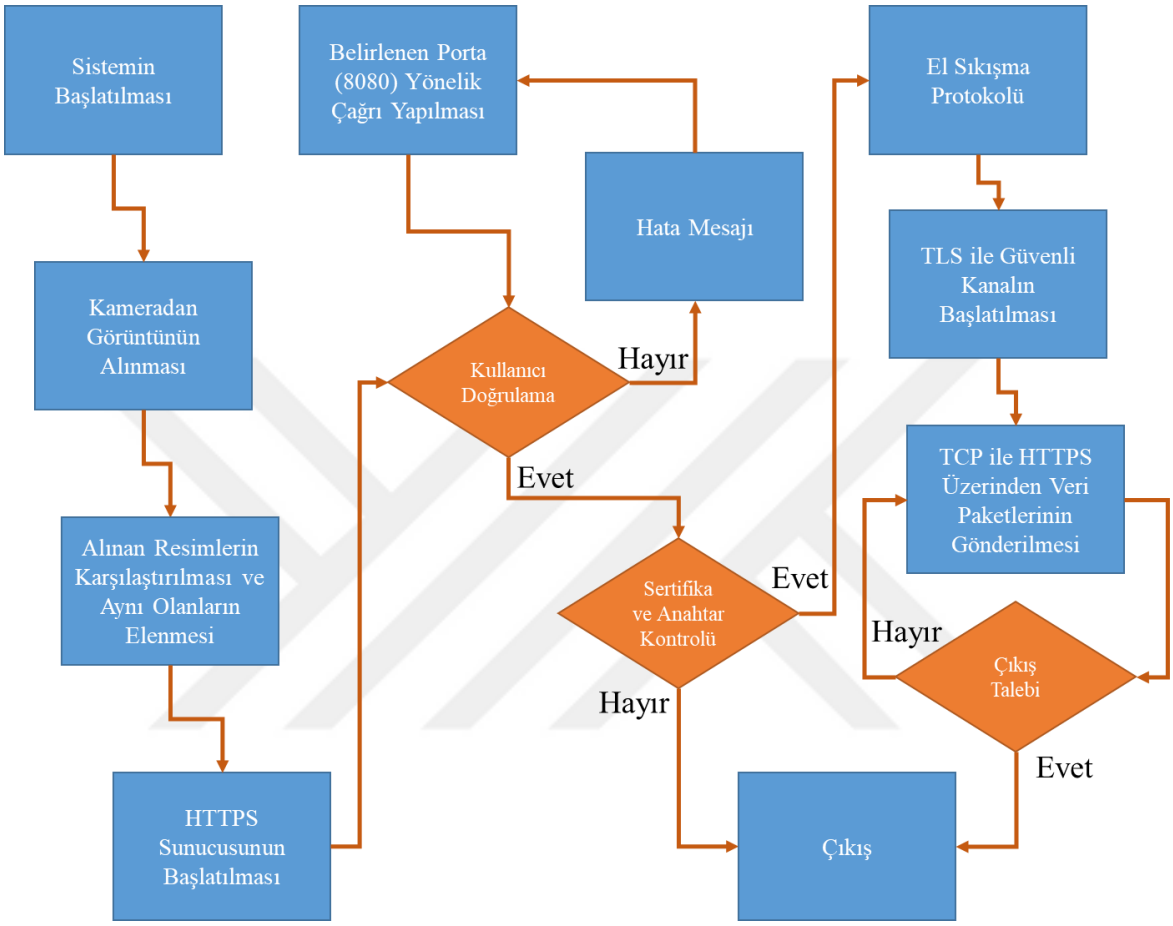
Google mühendisleri tarafından 2007 yılından itibaren geliştirilmeye başlanan açık kaynak kodlu programlama dilidir. Derlenmiş ve statik tipli bir dildir. Kasım 2009'da çıkmıştır. Go derleyicisi "gc", açık kaynak yazılım olarak, Linux, OS X, Windows, bazı BSD ve Unix versiyonları, ve ayrıca 2015'ten itibaren akıllı telefonlar için geliştirilmiştir [66]. Basitliği, güvenilirliği, çok hızlı derleme zamanı, derlendiğinde sadece bir binary file (exe dosyası) yaratması ve arkasında Google gibi bir destekleyicisi olması dilin avantajları arasında sayılabilir. Görüntü aktarımı için yazılmış kodlar Ekler bölümünde sunulmuştur.

5.4. Hyper Text Transfer Protocol (HTTP) Üzerinden Motion-JPEG Aktarımı

Motion-JPEG (mjpg) ile video akış neredeyse tüm tarayıcılar tarafından desteklenmektedir. Hem bu yaygın destek, hem her kameradan kolayca elde edilebilmesi hem de işlemlerde sağladığı kolaylık nedeniyle bu yöntem tercih edilmiştir. Ayrıca, Transmission Control Protocol/Internet Protocol (TCP/IP) standartları kapsamında mjpg HTTP üzerinden gönderilirken “video for linux-2” modülünden ve Oleksandr Senkovych tarafından hazırlanmış go-webcam kütüphanesinden [67] de istifade edilmiştir.

İHA sistemlerinde güvenli görüntü aktarımına ilişkin geliştirilen yöntemin algoritması Şekil 5.2’de sunulmuştur. Sistemin başlatılması ile birlikte kamera da belirlenen çözünürlükte görüntü aktarımına başlamaktadır. Alınan resimler sırasıyla karşılaştırılmakta ve kameradan aynı resmin birden fazla gelmesi durumunda fazlalıklar elenmektedir. Elenmeyen resimler ise sunucuda oluşturulan byte tipinde “jpegimage” dizinine sırayla ve her seferinde bir tane olacak şekilde atanmaktadır. Dizindeki her bir jpeg görüntüye, kullanıcı bazında belirlenen bir resim veya metin filigran olarak eklenmektedir. İstemciden belirlenmiş porta (8080) yönelik gelen talep ile; öncelikle kullanıcı doğrulama ve yetkilendirme işlemi yapılmakta, giriş başarısız ise istemciye hata mesajı gönderilmekte, başarılı ise HTTPS sunucusunun başlatılmakta, ardından da sertifika ve anahtar kontrolü gerçekleştirilmektedir. Kontrolün başarısız olması durumunda istemci sistemden çıkarılmakta, başarılı olması durumunda ise el sıkışma protokolünün ardından Transport Layer Security (TLS) ile oluşturulan güvenli

kanal başlatılmaktadır. jpegimage dosyasına, belirlenen başlık (header) bilgisi de eklenerek istemciler tarafından alınabilecek şekilde oluşturulan veri paketleri, Aktarım Kontrol Protokolü (TCP) servisini kullanarak, HTTPS üzerinden sıra ile aktarılmaktadır.



Şekil 5.2. Güvenli görüntü aktarımına ilişkin geliştirilen yöntemin algoritması

İstemci yeni jpeg dosyasını almak istediği ve sunucu yeni jpeg dosyasını sağlamak istediği sürece TCP bağlantısı kapanmamaktadır. İstemci çıkış talebinde bulunduğunda sistemden çıkışı sağlanmaktadır. İstemcide;

- http://sunucu IP:8080/jpeg adresi ile sadece bir resim (JPEG),
- http://sunucu IP:8080/mjpeg adresi ile görüntü (mjpg) alınabilmektedir.

Hazırlanan ortamda; birden fazla istemci (bilgisayar, tablet veya akıllı telefon) eş zamanlı olarak web tarayıcı veya VLC player üzerinden resim veya görüntü alabilmekte, modem ayarlarında yapılacak düzenleme ile resim/görüntü internete aktarılabilmektedir.

5.4.1. Motion-JPEG

Mjpg, dijital kameralar, IP kameralar ve web kameraları gibi video yakalama cihazları tarafından kullanılan ve her video karesi ayrı bir jpeg görüntüsü olan video sıkıştırma formatıdır. QuickTime Player, PlayStation konsolu ile Safari, Google Chrome, Mozilla Firefox ve Microsoft Edge gibi web tarayıcıları tarafından desteklenmektedir. Resimler birbirinden bağımsız olarak sıkıştırıldığından, mjpg, donanım aygıtlarında daha düşük işlem ve bellek gereksinimine ihtiyaç duyar. Video akışında meydana gelen hızlı değişimleri kolayca tolere edebilmektedir [68].

5.4.2. Video for linux-2 (v4l2)

V4l sunucu modülü, HTTP veya HTTPS protokolleri üzerinden kameradan gelen görüntüye gerçek zamanlı olarak herhangi bir tarayıcı tarafından erişilmesini sağlayan Linux'e özgü bir eklentidir. V4l yakalama, aktarma ve yayımlama için çeşitli kamera ve video aygıtlarının kullanılmasını sağlar. Video akışını görmeyi ve kamera ayarlarını tam olarak kontrol etmeyi sağlayan bir Web arayüzünü sunar. Ayrıca güvenli HTTPS protokolü dışında normal ve yönetici kullanıcıları için temel kimlik doğrulama işlevini de destekler.

5.4.3. Transmission control protocol/Internet protocol yapısı

TCP/IP, bir ağ üzerinden yapılan iletişimi yöneten kurallar kümesidir. Bu protokoller, kaynak ve hedef veya internet arasındaki verilerin hareketini tanımlar. HTTP TCP IP trafiğini desteklemektedir. Bağlantı odaklı olması, yüksek güvenilirlik gerektiren uygulamalar için uygundur olması, aktarılan verilerin bozulmadan ve gönderildiği sırayla gideceği garantisi bulunması, Akış Kontrolü ve Hata Kontrolü/Düzeltme yapması nedenleri ile TCP kullanımı tercih edilmiştir.

5.5. Yazılımda Yapılan Geliştirme ile Görüntü Aktarımının Etkinleştirilmesi

Oluşturulan ortamda geliştirilen güvenli görüntü aktarım metodu uygulamalarında; ağ üzerinden aktarılan resim sayısı ile kameradan alınan resim sayısı arasında resmin çözünürlüğüne bağlı olarak fark olduğu tespit edilmiştir. Kamera modülü özelliği gereği yine çözünürlüğe bağlı olarak saniyede 60 görüntüden (fps-frame per second) fazlasını

gönderemesine rağmen ağ üzerinden saniyede aktarılan resim sayısının düşük çözünürlüklü 1.200'e ulaştığı belirlenmiştir.

Kodda yapılan bir düzenleme ile; frame_say ve gonderme_say adında iki değişken tanımlanmış, frame_say ile kameradan gelen resimler sayılmış ve numaralandırılmış, gonderme_say değişkeni ile de ağ üzerinden aktarılan resimler sayılmış ve numaralandırılmıştır. İkinci safhada, frame_say ile gonderme_say değişkenleri vasıtası ile resimler karşılaştırılmış ve kameradan gelen resimde değişiklik olması durumunda jpegimage" dizinine atanmış, değişiklik olmadığı durumda ise resmin ağ üzerinden aktarılmaması sağlanmıştır.

Yapılan uygulamalarda/denemelerde 30 fps esas alınmış ve incelemeler/karşılaştırmalar sonucunda elde edilen aktarılan resim miktarı karşılaştırması Çizelge 5.1'de sunulmuştur. Tabloda görüldüğü üzere; yüksek çözünürlüklü resimlerde ağ üzerinden aktarım sayısı yarı yarıya (1/2) azalırken düşük çözünürlükte bu oran kırkta bir (1/40) mertebesine kadar düşmüştür. 2592x1944, 2368x1656 ve 2144x1368 çözünürlükteki resimler ise özelliklerinde ifade edilmesine rağmen Raspberry Pikamera Modülü tarafından sağlanamamıştır

Çizelge 5.1. Aktarılan resim miktarı karşılaştırması

Çözünürlük	Geliştirme Öncesi (fps)		Geliştirme Sonrası (fps)		Fark
	Pikamera (fps)	Aktarılan (fps)	Pikamera (fps)	Aktarılan (fps)	
2592 x 1944	-	-	-	-	-
2368 x 1656	-	-	-	-	-
2144 x 1368	-	-	-	-	-
1920 x 1080	30	60	30	30	30
1600 x 900	30	70	30	30	40
1280 x 720	30	75	30	30	45
960 x 540	30	80	30	30	50
640 x 360	30	90	30	30	60
320 x 180	30	150	30	30	120
160 x 90	30	450	30	30	420
80 x 45	30	1200	30	30	1170

Yazılımda yapılan bu düzeltme ile sistemin etkinliğinin geliştirilmesi kapsamında;

- Aynı resmin birden fazla gönderilmesi engellenmiş, böylece aktarılan resim sayısı ve paralelinde veri trafiği de benzer şekilde azaltılmış,
- CPU (Central Process Unit-Merkezi İşlem Birimi) kullanımı ve paralelinde ihtiyaç duyulan donanım özelikleri düşürülmüş,
- Oluşturulan kablosuz ağın kapasitesine bağlı olarak görüntü aktarımından istifade edebilecek istemci bağlantı sayısı artırılmış,
- Saniyede aktarılan resim, 30 fps olarak sabitlenmiştir.

Bahsedilen geliştirmeleri gösterebilmek açısından, yapılan düzenleme öncesi ve sonrasında aktarılan veri miktarı karşılaştırması Çizelge 5.2'de sunulmuştur. Aktarılan resim sayısındaki değişiklik kapsamında burada da görüldüğü üzere; yüksek çözünürlüklü resimlerde ağ üzerinden aktarım miktarı yarı yarıya (1/2) azalırken düşük çözünürlükte bu oran kırk dörtte bir (1/44) mertebesine kadar düşmüştür.

Çizelge 5.2. Aktarılan veri miktarı karşılaştırması

Çözünürlük	Resim Boyutu (kb)	Geliştirme Öncesi (fps)		Geliştirme Sonrası (fps)		Fark (mb/s)
		Aktarılan (fps)	Aktarılan Veri (mb/s)	Aktarılan (fps)	Aktarılan Veri (mb/s)	
2592 x 1944	609	-	-	-	-	-
2368 x 1656	524	-	-	-	-	-
2144 x 1368	456	-	-	-	-	-
1920 x 1080	370	60	21,67	30	10,80	10,87
1600 x 900	289	70	19,75	30	8,46	11,29
1280 x 720	211	75	15,45	30	6,18	9,27
960 x 540	137	80	10,70	30	4,01	6,69
640 x 360	77	90	6,76	30	2,25	4,51
320 x 180	25	150	3,66	30	0,73	2,93
160 x 90	8	460	3,59	30	0,23	3,36
80 x 45	3	1200	3,51	30	0,08	3,43

5.6. Veri Aktarımı İçin Şifreli Kanal Oluşturulması ve Verilerin Kriptolu Aktarımı

Beşinci bölümde de bahsedildiği üzere; video dosyalarının işlenmesi büyük miktarda veri hacmi doğurur, şifreleme için ise yazılımsal ve donanımsal gereksinim ile ihtiyaç duyulan süreyi artırır. Video sistemi ve hava aracı, sınırlı bataryayı ve teknik donamımı paylaşmak zorunda olduğundan ayrıca büyük video verisi ve sınırlı kaynaklar arasında ciddi uyumsuzluk oluşturduğundan şifreleme düzeni mümkün olduğunca basit tasarlanmalıdır. Bu durum da güvenlikten ödün verilmesi sonucunu doğurmaktadır. Bu nedenle İHA'lar için geliştirdiğimiz güvenli görüntü aktarım yönteminde verilerin ayrı ayrı şifrelenmesi yerine kanalın şifrelenerek verilerin bu güvenli kanal üzerinden yer kontrol istasyonuna aktarılması esas alınmıştır. Bu yöntemin izlenmesinin sağladığı faydalar şunlardır:

- Hava aracı üzerinde bulunan kısıtlı donanımdan (uçuş bilgisayarı, video sistemi, batarya vb.) istifade ederek ilave donanım ihtiyacı gereksinimi ortadan kaldırmak ve İHA'nın kaldırma kapasitesini aşmamak ya da uçuş süresini düşürmemek,
- Hava aracı üzerinde bulunabilecek birden fazla kameradan alınacak veriler ile diğer uçuş verilerinin (telemetre) ayrı ayrı şifrelenmesi yerine tüm verileri zaten şifrelenmiş ve güvenliği sağlanmış bir kanal üzerinden göndermek,
- Benzer şekilde, yer kontrol istasyonunda da donanım ihtiyacını asgari seviyede tutmak ve hava aracına verilecek komutları da oluşturulan güvenli kanal üzerinden hava aracına göndermek,
- İki taraflı veri aktarımında verilerin ayrı ayrı şifrelenmesi için gerekli zamanı azaltarak görüntü aktarımında yaşanması muhtemel gecikmeleri ve dolayısı ile yapılabilecek hayati hataları (koordinata dayalı hedef tespiti, hedefin ateş altına alınması vb.) ortadan kaldırmak.

Yukarıda izah edilen nedenlerle güvenli kanalın oluşturulabilmesi için Aktarım Katmanı Güvenliği TLS protokolünün kullanılması tercih edilmiştir.

5.6.1. Transport layer security

Ağ üzerinden iletişim kuran tarafların kimliğini doğrulamak için açık anahtar (asimetrik şifreleme) altyapısına dayalı sayısal sertifikalar kullanan bir güvenlik protokolüdür.

Sunucunun kimliğini bir sertifika ile istemciye göndermesi ve istemcinin sunucunun kimliğini doğrulaması esas alınır. Burada protokolün iki temel avantajı söz konusudur; şifreleme ve kimlik doğrulama. TLS, el sıkışma (Handshake) protokolü ile istemci, sunucudan güvenli bir bağlantı isteğinde bulunur, sunucu, istemciye sertifikasıyla (X.509 sertifikaları) birlikte açık anahtarını gönderir, istemci, sertifikanın güvenilirliğini kontrol eder, rastgele bir simetrik şifreleme anahtarı üretir ve sunucunun açık anahtarını kullanarak şifrelediği simetrik şifreleme anahtarını sunucuya gönderir, sunucu, kendi açık anahtarıyla şifrelenmiş olan bu mesajı çözerek simetrik anahtarı elde eder. Böylelikle güvenli bağlantı sağlanmış olur ve bu simetrik anahtarı kullanarak AES-256 standardı ile şifrelenen veriler karşılıklı gönderilir [69].

5.6.2. Kullanılan sertifika

TLS protokolü kapsamında kullanılmak üzere anahtar ve sertifika dosyaları oluşturulmuştur: 'cert.pem' ve 'key.pem'. Sertifika kendinden imzalı ve X.509 standardındadır. Ancak arzu edilmesi durumunda bir Sertifika Otoritesi (Certificate Authority-CA) tarafından üretilmiş sertifika da temin edilerek kullanılabilir.

Gizliliği artırılmış posta (Privacy enhanced mail-PEM), 1993 yılında geliştirilmiş ortak anahtarlı şifreleme yöntemini kullanarak e-postaları güvence altına alınması yöntemidir. Halen anahtar ve X.509 sertifikalarını saklamada yaygın olarak kullanılmaktadır [70].

X.509 ise kriptografide, dijital sertifika ve ortak anahtar şifrelemesini yönetmek için kullanılan önemli bir standarttır. web ve e-posta iletişimini güvenli hale getirmek için kullanılan TLS protokolünün önemli bir parçasıdır. Bir standart olarak X.509; genel anahtar sertifikaları, sertifika iptal listeleri, öznitelik sertifikaları ve bir sertifika yolu doğrulama algoritması için formatları belirtir [71].

Geliştirilen güvenli görüntü aktarım yöntemini için oluşturulan anahtar ve sertifikaya ilişkin özellikler Çizelge 5.3’de sunulmuştur.

Çizelge 5.3. Anahtar ve sertifikaya ilişkin özellikler

Sürüm	Sürüm 3
Seri Numarası	00:AB:DE:C5:BA:08:8B:17:DE
Sertifika İmza Algoritması	SHA-1 (RSA Şifrelemeli)
Yayıncı	E (e-posta) : icuhadar@gmail.com CN (genel isim) : 192.168.1.103 OU (kurumsal birim) : UAV O (kurum) : ISMET L (konum) : CANKAYA ST (şehir) : ANKARA C (ülke) : TR
Geçerlilik	Başlangıç: 16 Aralık 2017 Cumartesi 22:39:19 Bitiş: 17 Aralık 2017 Pazar 01:39:19
Özne Genel Anahtar Algoritması	RSA Şifrelemesi
Özne Genel Anahtarı	(2048 bit): D6:22:5B:28:4F:6F:A3:EA:81:F1:3A:C3:01: 00:E9:61:64:BF:E8:40:69:D5:18:97:E8:B8:A0:02:C7:50 :23:B0:61:57:3C:58:43:ED:77:C7:C7:38:7F:95:E3:A9:F 4:D4:14:E1:FE:7A:76:FE:9B:07:A1:68:31:E1:F0:27:30: 49:C3:75:76:68:2E:B7:89:84:D1:E0:60:57:BF:0E:C4:F1 :47:8F:50:AA:F7:18:38:8E:79:B0:3A:E7:A9:47:07:9C: A1:15:76:B0:41:FA:FB:7B:EC:16:4D:32:2E:60:45:B8:9 4:73:51:0E:06:A1:CA:D3:A8:D0:F3:B8:31:8F:8C:0D:0 8:25:82:BA:5F:E0:03:8D:05:CA:2D:31:B7:09:FF:1C:72 :93:37:28:DA:C0:23:41:4F:8C:95:96:9E:B0:2A:AA:D3: 48:64:F4:11:E2:1C:CD:33:2D:3B:64:2D:9A:D8:89:9A: 3A:7E:4A:E2:9A:CD:AB:AB:A4:8F:E8:58:90:E3:10:B C:E3:83:C9:34:4C:F8:A5:B0:5B:19:BB:5C:F9:82:A5:5 7:93:A6:71:99:4B:CA:3C:03:B1:BF:47:DD:8A:DC:B9: E6:08:E9:7D:6F:86:B3:8B:43:BD:1C:A9:FB:35:25:05:1 3:93:9A:32:20:52:15:82:40:FE:8F:CA:FB:44:CA:53
Sertifika Konu Anahtar Kimliği	Boyut: 20 bayt / 160 bit F1:13:C1:AB:78:D0:3D:41:91:98:51:2E:38:00:79:46:59 :B4:BC:1C
Sertifika Makamı Anahtar Kimliği	Boyut: 9 bayt / 72 bit 00:AB:DE:C5:BA:08:8B:17:DE

Çizelge 5.3. (devam) Anahtar ve sertifikaya ilişkin özellikler

Sertifika İmza Değeri	Boyut: 256 bayt / 2048 bit 80:7B:A8:64:90:9E:39:C0:2C:12:88:AE:A5:6C:03:69:7 C:B1:99:E9:CC:56:A7:AB:61:F8:4D:37:6B:E4:DB:F8:7 F:22:C4:8F:91:76:DF:02:A2:B8:C5:E1:81:B5:6C:8A:04 :85:06:A6:F7:54:97:73:6F:36:FD:A3:E7:6F:DF:53:E4:1 5:05:3F:AC:8B:27:47:16:60:F1:37:04:71:59:FF:E6:7B: A1:76:47:A4:CC:8B:B9:3D:B5:C6:58:4F:02:F8:64:78:1 3:39:0A:85:A4:1B:92:4B:73:F5:44:02:C5:63:0B:0F:31: 6A:2C:BC:2E:9E:04:22:6E:D7:49:F8:3E:EE:E8:52:6B: 6A:A2:58:76:CD:E7:65:FA:F5:6F:EF:A9:AD:A4:C1:D 3:1D:22:49:08:72:9B:71:C8:74:61:CF:60:D7:BF:0A:F7: 94:E2:D4:B7:F7:AF:38:4F:E7:12:D4:5D:91:12:CD:83: EC:25:25:DF:EB:DC:64:F0:69:E3:5F:19:59:54:DB:18: CE:B5:3A:2B:56:36:E5:7B:4E:5B:C5:AA:E3:93:C7:CC :40:9F:6D:FA:50:B2:6B:86:5F:86:D8:62:AC:D3:0D:05: C8:3B:AB:E9:C4:05:B4:E0:46:31:D7:EA:5D:F6:2A:14: 34:C2:58:DE:09:39:97:48:DD:82:F3:B0:72
Ortak Anahtar	RSA (2048 bit): 30:82:01:0A:02:82:01:01:00:D6:22:5B: 28:4F:6F:A3:EA:81:F1:3A:C3:01:00:E9:61:64:BF:E8:4 0:69:D5:18:97:E8:B8:A0:02:C7:50:23:B0:61:57:3C:58: 43:ED:77:C7:C7:38:7F:95:E3:A9:F4:D4:14:E1:FE:7A:7 6:FE:9B:07:A1:68:31:E1:F0:27:30:49:C3:75:76:68:2E: B7:89:84:D1:E0:60:57:BF:0E:C4:F1:47:8F:50:AA:F7:1 8:38:8E:79:B0:3A:E7:A9:47:07:9C:A1:15:76:B0:41:FA :FB:7B:EC:16:4D:32:2E:60:45:B8:94:73:51:0E:06:A1: CA:D3:A8:D0:F3:B8:31:8F:8C:0D:08:25:82:BA:5F:E0: 03:8D:05:CA:2D:31:B7:09:FF:1C:72:93:37:28:DA:C0:2 3:41:4F:8C:95:96:9E:B0:2A:AA:D3:48:64:F4:11:E2:1C :CD:33:2D:3B:64:2D:9A:D8:89:9A:3A:7E:4A:E2:9A:C D:AB:AB:A4:8F:E8:58:90:E3:10:BC:E3:83:C9:34:4C:F 8:A5:B0:5B:19:BB:5C:F9:82:A5:57:93:A6:71:99:4B:C A:3C:03:B1:BF:47:DD:8A:DC:B9:E6:08:E9:7D:6F:86: B3:8B:43:BD:1C:A9:FB:35:25:05:13:93:9A:32:20:52:1 5:82:40:FE:8F:CA:FB:44:CA:53:02:03:01:00:01
Parmak İzleri	SHA-256 : B0:49:B9:5B:5D:0F:B7:46:54:A4:B6:C8:34:F2:5F:A7:2 3:56:D4:25:45:BB:68:EC:0C:29:4A:EE:81:8F:B8:72 SHA1 : A3:71:89:09:1A:A7:68:78:09:08:C2:F9:D2:C7:7C:9C:4 2:50:89:6D

5.7. Geliştirilen Arayüz ve Kullanıcı Giriş Sistemi

İHA'dan alınan video görüntüsü ve istenirse uçuş bilgilerini (telemetre) de kapsayan tüm verilerin geliştirilen yöntem ve oluşturulan sertifikaya dayalı şifreli bir kanal üzerinden nasıl gönderileceği yukarıda açıklanmıştır. Özellikle; Man-in-the-Middle Attack

(Aradaki/ortadaki adam saldırısı) olarak adlandırılan, bir ağ üzerinde bilgisayarlar arası veya diğer ağ araçları arasına girerek veri paketlerini yakalamaya dayanan bir saldırı çeşidine karşı tedbir getirilmeye çalışılmıştır. Bu bölümde ise istemci tarafından güvenli ağa, güvenli ve kontrollü bir şekilde bağlanılması için oluşturulmuş arayüz ve özelliklerinden bahsedilecektir.

5.7.1. Arayüz

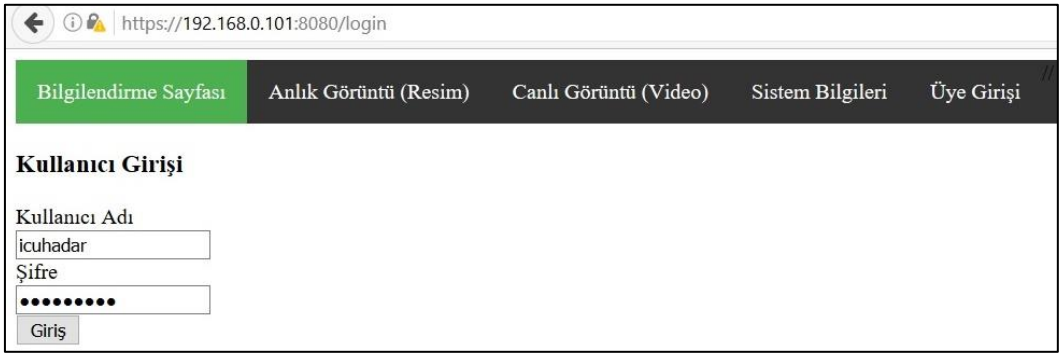
İHA görüntüsünün izlenebilmesi için ihtiyaç duyulan her kullanıcıya ayrı giriş yetkisi verilmesi esas alınmıştır. Yine güvenliğin sağlanabilmesi adına arayüz üzerinden yeni kullanıcı hesabı oluşturulmasına müsaade edilmemiştir. Bu maksatla sunucudaki veri tabanında kullanıcı hesaplarına ilişkin Çizelge 5.4'deki bilgiler tutulmaktadır.

Çizelge 5.4. Kullanıcı hesap bilgileri

Sıra No.	Kullanıcı Adı	Şifre	Ad Soyad	IP*	Koordinat* (GPS verisi)
1	icuhadar	icuhadar1	İsmet ÇUHADAR		
2	mdursun	mdursun1	Mahir DURSUN		
3	user	password	Tanımlanmamış		

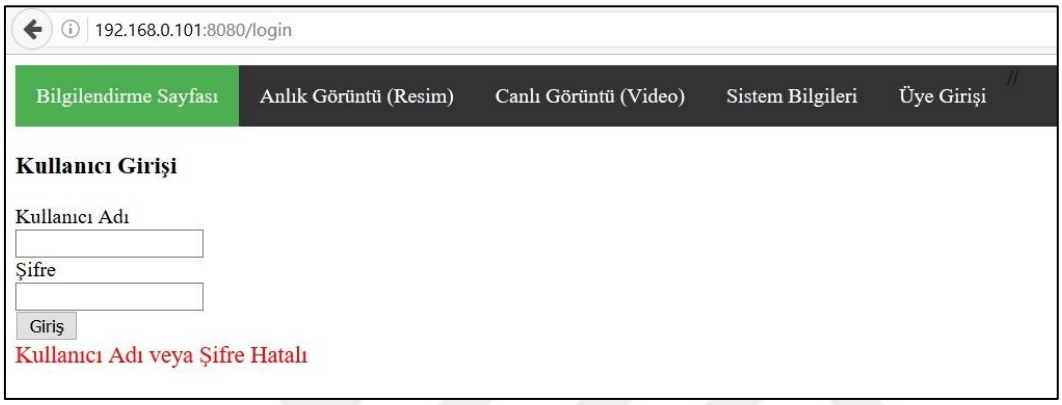
* Statik IP kullanılmadığından ve geliştirme ortamında GPS bulunmadığından aktif değildir; gerçek İHA görüntüsü aktarımında kullanılmak üzere dahil edilmiştir.

İstemcide, "http://sunucu IP:8080" veya aktif ise "https://sunucu IP:8080" adresi yazılarak ilgili web sayfası çağırıldığında Resim 5.6'daki kullanıcı giriş arayüzü istemcinin tarayıcısında görülecektir.



Resim 5.6. Kullanıcı giriş arayüzü

Bu arayüzde Çizelge 5.4'te belirtilen şekilde tanımlanmış kullanıcıların veri tabanındaki "kullanıcı adı" ve "şifre" bilgilerini doğru girmeleri beklenmektedir. Önceden tanımlanmamış kullanıcının da önceden tanımlanmış ancak "kullanıcı adı" ve/veya "şifre" bilgisini yanlış yazmış kullanıcının da sisteme girmemesi garanti edilmiştir. Bu durumda Resim 5.7'deki arayüzdeki gibi kullanıcı giriş hatasını belirten bir mesaj ile karşılaşılacaktır. Başarılı bir kullanıcı girişi yapılmadan sunucudan görüntü aktarımı başlamamaktadır.



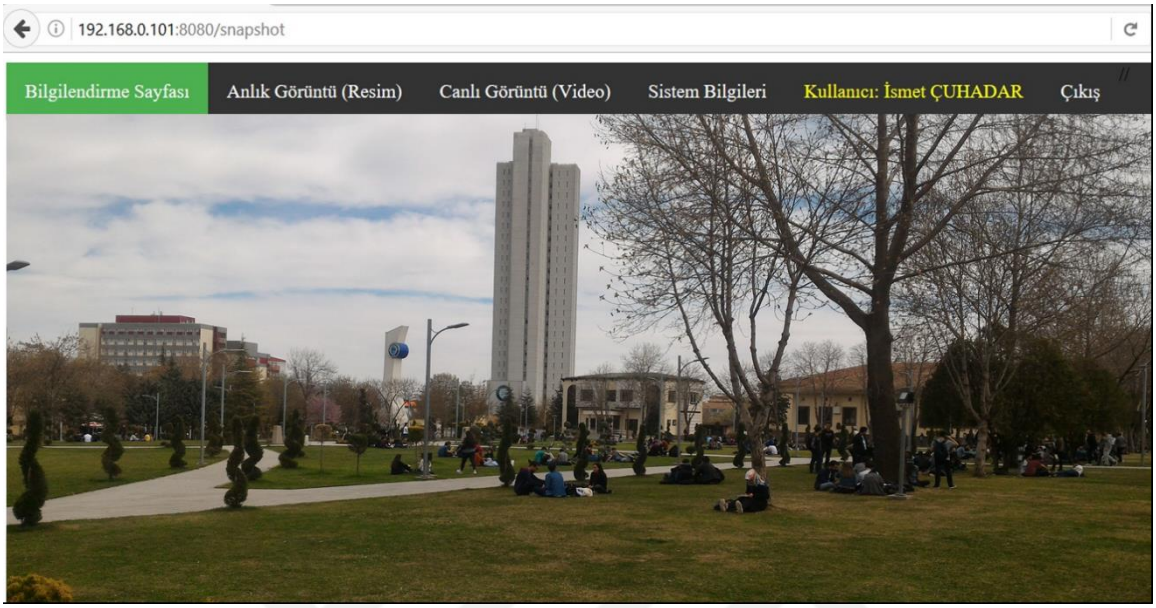
Resim 5.7. Kullanıcı giriş hatasını belirten mesaj

Tarayıcıda ilgili web sayfası ilk açıldığında yani kullanıcı girişi yapılmadan önce, Resim 5.8'de görüldüğü üzere beş ayrı sekmeden oluşan kullanıcı arayüzü ile karşılaşılmaktadır:

- Bilgilendirme Sayfası: projeye ilişkin bilgileri sunmak,
- Anlık Görüntü (Resim): kameradan tek resim almak,
- Canlı Görüntü (Video): kameradan canlı görüntü akışını sağlamak,
- Sistem Bilgileri: sisteme ilişkin ihtiyaç duyulan bilgileri paylaşmak,
- Üye Girişi: kullanıcı girişi yapmak için kullanılmak üzere.

Resim 5.8. Beş ayrı sekmeden oluşan kullanıcı arayüzü

Kullanıcı girişi yapılmasını müteakip açılan sayfa ve görülen arayüz Resim 5.9'da sunulmuştur.



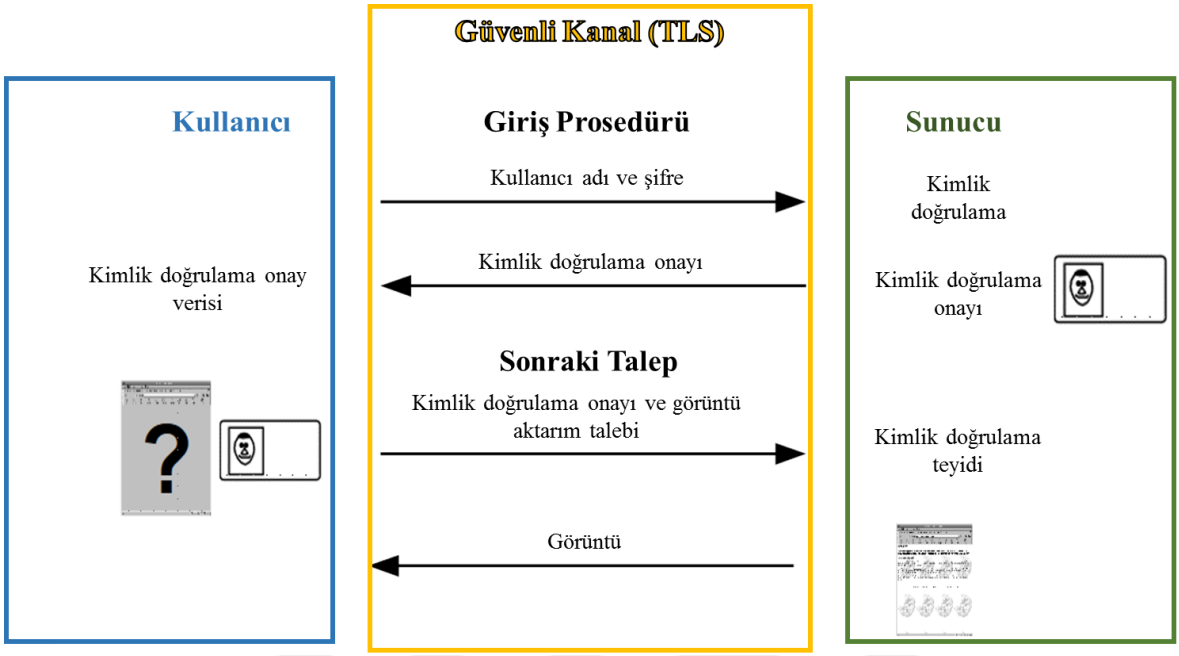
Resim 5.9. Kullanıcı girişi yapılmasını müteakip açılan sayfa ve görülen arayüz

Başarılı kullanıcı girişi ile birlikte arayüzdeki sekmelerde de değişim meydana gelmektedir. "Üye Girişi" yerine zaten kullanıcı girişi yapılmış olduğundan "Çıkış" sekmesi belirmektedir. Ayrıca giriş yapan kullanıcı ve şifresi karşılığında veri tabanında tutulan personel ad ve soyad bilgileri de arayüzün üstündeki şeritte görülebilmektedir.

5.7.2. Kullanıcı giriş sistemi güvenlik özellikleri

Kullanıcının sisteme girişi, kimlik doğrulaması ve neticesinde görüntü aktarımının nasıl yapıldığını içeren kullanıcı giriş sistemi genel hatları ile Şekil 5.3'de görülmektedir. Kullanıcı adı ve şifresinin, istemci tarafından oturum başında sunucuya gönderilmesi ve sunucunun bu verileri doğrulaması esas alınmış ve bu işlemin güvenli olarak yapılabilmesi için kullanıcı adı ve şifresinin güvenli kanaldan, yani TLS üzerinden şifrelenerek gönderilmesi, böylece istenmeyen kişilerce elde edilememesi amaçlanmıştır. Kullanıcı tarafından çıkış yapılmadığı ve sunucu tarafından kapatılmadığı sürece görüntü aktarımı devam etmektedir. İstemci aynı olsa dahi her oturum açılışında/yenilenişinde tekrar kullanıcı adı ve şifresi istenmektedir. Arayüz üzerinden yeni kullanıcı hesabı oluşturulmasına müsaade edilmeyerek kullanıcı sayısı kontrol altında tutulması, Böylelikle sadece sunucu

üzerindeki veri tabanında belirlenen kullanıcıların görüntü aktarımını görebilmesi hedeflenmiştir.



Şekil 5.3. Kullanıcı giriş sistemi [72]

Bazı servis engelleme (Denial of Service) saldırılarında, saldırganlar sunucuya bağlantı yapmakta, herhangi bir bilgi göndermen zaman aşımı süresine kadar bekletebilmekte, benzer bağlantının sayısı artırılarak sunucu kaynakları gereksiz harcanabilmektedir. Görüntü aktarımının, yalnızca doğru kullanıcı adı ve şifresi girilmesi ile başlatılması neticesinde bu tip saldırıların da önüne geçilmesi ve sunucu kaynaklarının verimli kullanımı [73] sağlanmaktadır. Kaç istemci ve kaç kullanıcı girişi olursa olsun tüm giriş ve çıkışlar (oturum açılış ve kapanışları) zamanı (tarih ve saat olarak) ve IP adresi ile birlikte sunucuda kayıt altında tutulmaktadır (loglanmaktadır). Sunucu, kullanıcı adı ve şifreyi doğruladıktan sonra tarayıcının kimlik doğrulamasının yapıldığını, rastgele üretilen süreli bir çerezde (cookie) saklamakta ve oturum verisi olarak referans vermek için bu çerezi kullanılmaktadır. Kimlik doğrulaması yapıldığı bilgisi güvenlik açısından yalnızca sunucu veri tabanında tutulmaktadır.

6. GÖRÜNTÜ AKTARIM METODLARININ RİSK TABANLI ÇOK KRİTERLİ KARAR VERME YÖNTEMİ KULLANILARAK KARŞILAŞTIRILMASI

Bu bölümde esas olarak, İHA'larda güvenli veri aktarımı için geliştirilen yöntemin, literatür taraması neticesinde tespit edilen diğer yöntemlerle karşılaştırılarak güvenlik açısından getirdiği artılar ve diğer olumlu hususların tespit edilmesi hedeflenmektedir. Bu amaçla; "Risk Yönetimi" ve "Çok Kriterli Karar Verme" yöntemleri birleştirilerek yeni ve özgün bir yöntem ortaya konulmaya çalışılmıştır: "Risk Tabanlı Çok Kriterli Karar Verme". Yöntemin anlaşılabilmesi için "Risk Yönetimi" ve "Çok Kriterli Karar Verme" yöntemlerine kısaca değinilecek ve müteakiben karşılaştırma yapılacaktır. Ancak bu çalışmada asıl maksat yöntemleri güvenlik açısından karşılaştırmak olduğundan risk yönetiminin sadece ilk iki aşaması olan "Risk (tehlike) tanımlaması" ve "Risk değerlendirmesi (risk analizi)" uygulanacaktır. Bu bölümde göz önünde bulundurulması gereken bir diğer önemli husus da risk tanımlama ve analizinin İHA'nın tamamı için değil sadece veri linkine yönelik yapılacak olmasıdır.

6.1. Risk Yönetimi

Güvenli bir tasarım elde etmek için, tehlikelerin elimine edilmesi veya azaltılması şarttır. Risk yönetimi; risklerin tanımlanması, değerlendirilmesi, önlem alınması, izlenmesi ve iletişim çerçevesinin tesisi gibi bazı hususları içermektedir. Bu süreçte tehlikelerin belirlenmesi kritik bir sistem güvenliği fonksiyonudur [74].

6.1.1. Risk yönetimi işlem basamakları

Bu konuda farklı yaklaşımlar bulunmakla birlikte ana maddeler konusunda bir uyumluluk söz konusudur. Genel olarak ifade edilirse, risk yönetimi beş aşamadan oluşan ve tekrar eden bir döngüdür. Risk yönetim modeli işlem basamakları Şekil 6.1'de sunulmuştur. Bu döngüde asıl maksat; risklerin belirlenmesi, mümkünse ortadan kaldırılması, değil ise olasılık ya da şiddetinin azaltılarak riskin kabul edilebilir seviyeye getirilmesidir.

Şekil 6.1. Risk yönetim modeli işlem basamakları [75]

Risk (tehlike) tanımlaması; kayıp veya zarara neden olabilecek potansiyele sahip her unsurun tespitini gerektirmektedir. Bu aşamada tüm risk/tehlikeler ortaya çıkartılmalıdır. Risk yönetiminin en kritik aşamasıdır. Risk değerlendirmesi (risk analizi) aşamasında; bir önceki basamakta tespit edilen riskler, olasılık ve sonuç bakımından karşılaştırılır ve bir sıralamaya tabi tutulur. Risk azaltma ve risk kararının verilmesi sürecinde; olasılık ve sonuçları bakımından sıralanan riskler, kabul edilebilirlikleri açısından önceden tesis edilmiş kriterler ile kıyaslanır ve eylem gerektirip gerektirmediği hakkında karar verilir. Kontrol tedbirlerinin uygulanması aşamasında; önceki aşamada tedbir alınması gereken risk olarak belirlenen hususlar için atılması gereken adımlar ortaya konur ve uygulanır. Son aşama olan denetleme ve değerlendirmede ise; ilk safhada tespit edilen riskler ile kontrol tedbirlerinin uygulanması sonrası gelinen aşama karşılaştırılır, tedbirlerin uygunluğu kontrol edilir ve sürece ilk adımdan tekrar başlanır. Risk seviyesini etkileyecek muhtemel tüm faktörlerin gözden geçirilmesi önem arz etmektedir [74].

6.1.2. Temel tanımlar

Risk analizinin önemli bileşenleri olan kaza, aksilik, tehlike ve riske ilişkin temel tanımlar aşağıda sunulmuştur.

Kaza; malzeme, ekipman, kargo vb. unsurda hasara, yaralanmaya veya ölüme neden olan, planlanmamış, istenmeyen, beklenmeyen olaydır.

Aksilik; ölüm, yaralanma, meslek hastalığı, ekipman veya çevrede kayıp ve hasarlara neden olan planlanmamış olay, kazadır. Aksilik kazayı da içeren daha geniş bir çerçeveyi ifade etmektedir.

Tehlike; ölüm, yaralanma, meslek hastalığı, ekipman veya çevrede kayıp ve hasarlara neden olabilecek potansiyel veya gerçek durumdur. Kazanın ön şartıdır. Tehlike üç temel bileşeni içermektedir; "Tehlikeli Eleman (Hazardous Element-HE)", "Tetikleyici Mekanizma (Initiating Mechanism-IM)" ve "Hedef ve Tehdit (Target and Threat-TT)". Bu bileşenler "Tehlike Üçgeni" olarak da adlandırılmaktadır. Bunlardan birinin ortadan kalkması ile tehlike elimine edilmiş olmaktadır.

Risk; bir aksiliğin ortaya çıkma olasılığı ve şiddetinin ifadesidir. Tehlike ve aksilik, risk ile birbirine bağlanmaktadır [74].

Risk = Olasılık x Şiddet

6.1.3. Tehlikelerin belirlenmesi

Bu maksatla kullanılabilecek çeşitli yöntemler bulunmaktadır:

- Tehlike Üçgeni bileşenlerinin belirlenmesinde tehlikeli eleman çeklisti kullanılır.
- Bilinen tetikleyici mekanizmalarına yoğunlaşılır.
- Bilinen aksilik ve istenmeyen çıktılara önem verilir.
- Geçmiş deneyimler ve eğitimlerde edinilen bilgilerden yararlanılır.
- Başarılı tasarım uygulamaları incelenir.
- Genel tasarım güvenlik kriterleri, prensipleri ve kuralları gözden geçirilir.
- Tehlikeye neden olan ikinci seviye faktörler incelenir.
- Kilit başarısızlık durumlarına ilişkin sorulara cevap aranır [74].

6.1.4. Ön tehlike listesi (Primary hazard list-PHL)

Sistemde olabilecek potansiyel tehlike ve aksiliklerin belirlenmesi amacıyla kullanılan bir analiz tekniğidir. Devam eden tüm tehlike analizleri için bir başlama noktası niteliğindedir.

Burada tespit edilen tehlikeler daha detaylı tehlike analiz ve değerlendirme yöntemleri ile analiz edilir. Bu yöntemin birincil amacı potansiyel sistem tehlikelerinin tanımlanıp listelenmesi iken ikincil amacı ise kritik güvenlik faktörleri ve aksilik kategorilerinin tanımlanmasıdır. Temel niyet, geliştirmenin en erken aşamalarında tasarımı etkilemektir. Beyin fırtınası çalışmalarına benzer bir yaklaşımla tehlikeler öne sürülerek bilinen ve şüphelenilen tehlikelerin tamamı bir listede toplanır. Bu süreçte elde edilen en önemli çıktı tehlike çeklisti denilen bu listedir. Tehlikelere neden olan temel faktörler, üst seviye aksilik listesi ve kritik güvenlik faktörleri bu yöntem ile elde edilen diğer çıktılardır [74].

6.1.5. Ön tehlike analizi (Primary hazard analysis-PHA)

Sistem tasarımındaki tehlikelerin, onlara ilişkin nedensel faktörlerin, etkilerinin, risk seviyelerinin ve onları azaltacak tasarım ölçümlerinin tanımlanması amacıyla yapılan kalitatif bir güvenlik analizidir. Potansiyel tehlike analizi olarak da adlandırılır. Önceki safhalarda belirlenemeyen tehlikeler ile kritik güvenlik fonksiyonları ve üst seviye aksilikleri de belirler. En sık kullanılan analiz tekniğidir. Bu yöntemde; tehlikelerin tespit edilebilmesi maksadıyla "Güvenlik Blok Diyagramları" ve "Fonksiyonel Blok Diyagramları" kullanılmaktadır. Burada belirlenen tehlikelere yönelik olasılık ve şiddet tespit edilmekte, sonucunda da risk değerlendirme matrisi oluşturulmakta, bu verilerden de "Ön Tehlike Analiz Formunda" istifade edilmektedir. Burada belirlenen tehlikeler, risk değerlendirme matrisi ve analiz formunun yardımı ile sıraya konur ve önlemler öncelik sırasına göre alınır.

6.2. Karar Verme

İnsanlar/organizasyonlar, kişisel ve toplumsal ihtiyaçlarını karşılamak için sürekli karar verme kavramı ile karşılaşırlar. Karar, bir iş ya da sorun hakkında düşünülerek verilen kesin yargıdır. Karar verme ise, karar vericinin değişik alternatifler arasından, kendi amaçlarına uygun, kendisince önceden belirlenmiş belirli kriterlere göre en uygun alternatifi seçebilmesidir [76].

6.2.1. Karar teorisi

Karar verme işlemini analitik ve sistematik bir yaklaşımla incelemektedir. Karar teorisinde kullanılan matematiksel modeller, işletme yöneticilerine en iyi kararın verilmesinde

yardımcı olmaktadır. Bir problemin karar problemi olabilmesi için olabilmesi için aşağıdaki şartları birlikte sağlaması gerekmektedir:

- Birden çok davranış yolunun bulunması,
- Her bir davranışın sonuçlarının birbirinden farklı olması,
- Gerçekleştirilmek istenen birtakım amaçların olması.

İncelenen konunun kapsamına, karmaşıklığına ve önem derecesine göre karar verme eylemleri farklılık göstermesine rağmen temelde karar verme eylemlerinin ortak özellikleri aşağıda sunulmuştur:

- Alternatifler/seçenekler arasından seçim yapmayı gerektirir.
- Her karar verme eylemi bir amaca yöneliktir.
- Bir zaman sürecini gerektirir.
- Kararlar geleceği tahminlemeye dayanırlar.
- Karar verici, geleceğin belirsizliği nedeniyle bazı riskleri üstlenmek durumundadır [76].

6.2.2. Karar verme süreci

Karar, çeşitli aşamalardan geçerek oluşan bir süreçtir. Karar verme, karar vericinin değişik alternatifler ile karşılaşması durumunda bu alternatifler arasından kendi amaçlarına en uygun olanını seçme işlemi iken; karar süreci ise bu işlemlerin sırasıyla yapılmasını içerir. Karar verme sürecinin aşamaları şu şekilde sıralanabilir:

- Problemin farkına varma,
- Problemin belirlenmesi ve tanımlanması,
- Alternatiflerin belirlenmesi,
- Alternatiflerin değerlendirilmesi,
- En iyi alternatifin belirlenmesi,
- Kararın değerlendirilmesi

Karar verme sürecinde bu aşamaları geçerken izlenebilecek iki yaklaşım bulunmaktadır: kalitatif ve kantitatif. Kalitatif yaklaşım temel bilgi ve deneyime dayalı iken kantitatif

yaklaşım sayısal olgu ve verilere dayalıdır. Kalitatif karar verme, karar vericilerin sezgisel becerilerine bağlı olmasına karşılık, kantitatif karar verme yaklaşımında yöneylem araştırması kapsamındaki yaklaşım ve tekniklerin bilinmesini gerektirir [76].

6.2.3. Çok kriterli karar verme

Çok sayıda birbiriyle çelişen kriterin/tutumun söz konusu olduğu durumda alınan karar çok kriterli karar verme olarak bilinir. Oluşturulan kriterlere göre en uygun çözümü belirleme sürecidir. Belirgin sayıda ve özellikteki alternatif karşılaştırılarak derecelendirilir ve bunların arasından en iyisi seçilmeye çalışılır. Bu kapsamda, kriterlere ilişkin ağırlık bilgisi kullanılarak, çatışan niteliklere sahip karmaşık problemlerin çözülmesi hedeflenir. Tipik bir çok kriterli karar verme problemi üç temel bileşeni içerir:

- Alternatifler, bir problemdeki tercih seçenekleridir.
- Kriterler, alternatiflerin temel özellikleri, kaliteleri veya verimlilik parametreleridir.
- Her bir kriter için nisbi önemdir (ağırlıklar).

İlk olarak alternatiflerin ve niteliklerin tanımlaması yapılır. Sonrasında her bir alternatifin, tüm kriterlere göre ölçümleri elde edilir ve ağırlıkları atanır. Alternatiflerin bütünsel değerleri saptanır, sonuç önerileri ile değerlendirmeleri ortaya konulur. Sıklıkla kullanılan çok kriterli karar verme yöntemleri müteakip maddelerde kısaca açıklanmıştır [76].

Ağırlıklı toplam yöntemi

En çok bilinen ve en yaygın olarak kullanılan karar verme yöntemlerinden biridir. Bu yöntemde, her bir kritere göre alternatifin gerçek sayısal değeri, ağırlığı ile çarpılarak tüm kriterler için bu değerlerin toplamları alınır ve sonuç değerleri bulunur. Bu değerler arasından maksimumu sağlayan alternatif karar olarak seçilir.

Ağırlıklı çarpım yöntemi

Her bir alternatif, diğer alternatiflerle, her bir kriter için belirlenen oranla çarpılarak karşılaştırılır. Her bir alternatifin, başka bir alternatifle tüm kriterlere göre oranı alınır ve değerler üstel olarak ağırlıklandırılıp tüm kriterler için çarpılarak sonuç değerleri bulunur.

Analitik hiyerarşi prosesi (AHP)

Thomas L. Saaty (1980) tarafından geliştirilen AHP yöntemi karmaşık karar problemlerinde, alternatif ve kriterlere göreceli önem değerleri verilmek suretiyle, yönetsel karar mekanizmasının çalıştırılması esasına dayanır. En önemli özelliği karar vericinin hem objektif hem de sübjektif düşüncelerini karar sürecine dâhil edebilmesidir. Oluşturulacak hiyerarşik yapı üzerinden ikili karşılaştırmayı esas almaktadır.

PROMETHEE (Preference ranking organization method for enrichment evaluations)

Brans vd tarafından 1986 yılında geliştirilmiş olan yöntem diğer yöntemlere kıyasla, kavram ve uygulama bakımından daha kolay bir sıralama yöntemi içermektedir. Bu yöntem, birbiri ile çelişen birkaç kriterin göz önünde tutularak, sınırlı sayıda alternatifin sıralanmasının söz konusu olduğu problemlerde daha çok uygulanmaktadır. Alternatifleri farklı tercih fonksiyonları temelinde değerlendirerek alternatiflere ilişkin kısmi önceliklerin ve tam önceliklerin elde edilmesi ile ayrıntılı analizlerin yapılmasını sağlamaktadır.

ELECTRE (Elimination et choix traduisant la realité)

Roy tarafından 1971 yılında ortaya atılmış, daha sonra Nijkamp ve Van Delft ile Voogd tarafından geliştirilmiştir. Seçim gerektiren sorunların çözümü için tasarlanmıştır. Yönteminin esası, tercih edilen ve edilmeyen alternatifler arasında üstünlük ilişkisi kurulmasına dayanır. Üstünlük ilişkisinin kurulabilmesi için uyum ve uyumsuzluk indeksleri oluşturulur. Bu indeksler, hangi alternatifin daha baskın olduğunun seçilmesini sağlayan tatmin veya tatminsizliğin ölçüsünü gösterir. Her bir ölçüt için bir verimlilik bir de önem ölçüsü tespit edilir. Tayin
edilen verimlilik ölçüleri üzerinden her bir seçeneğe not verilir.

VIKOR (Vise kriterijumska optimizacija I kompromisno resenje)

Opricovic ve Tzeng tarafından 2004 yılında önerilmiştir. Uzlaşılmış bir sıralama belirlemeyi ve belirtilen ağırlıklar altında uzlaşılmış çözüme ulaşmayı sağlayan bir yöntemdir. Birbiri ile çelişen kriterler altında alternatiflerin sıralamasını belirleyerek en uygununun seçilmesini içerir ve ideal çözüme yakınlığa dayanan çok kriterli sıralama indeksini ele alır.

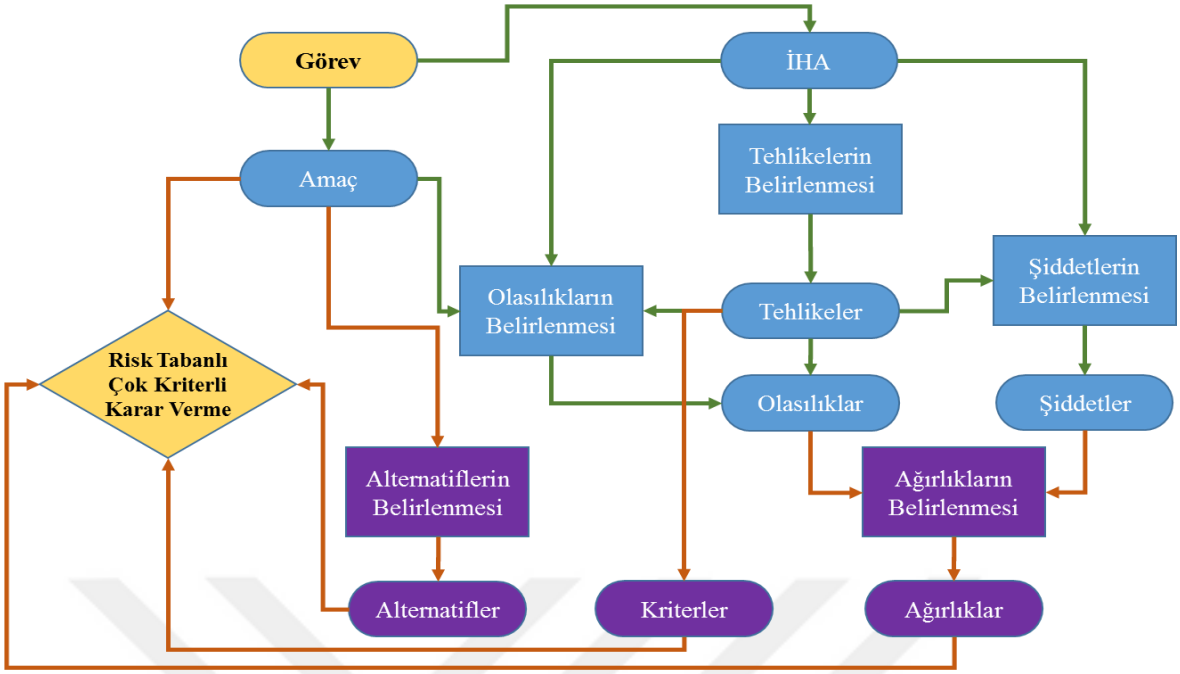
TOPSIS (Technique for order preference by similarity to ideal solution)

Yoon ve Hwang tarafından 1980 yılında geliştirilmiştir. ELECTRE yönteminin temel yaklaşımlarını kullanmaktadır. Alternatiflerin en iyi çözümü (pozitif ideal çözüme) görece yalınlıklarını dikkate alarak sıralanmasını sağlayan ve karar vericilere çözüm önerisi sunan bir yöntemdir. Pozitif ideal çözüm; ulaşılabilir bütün en iyi kriterlerin birleşimidir. Negatif ideal çözüm ise ulaşılabilir en kötü ölçüt değerlerinden oluşur. Seçilen alternatifin ideal çözüme yakınlığı belirlenirken bir o kadar da negatif ideal çözümden uzak olması beklenir [77].

6.3. Görüntü Aktarım Metotlarının, Risk Tabanlı Çok Kriterli Karar Verme Yöntemi Kullanılarak Karşılaştırılması

Bu bölümde açıklayacağımız çalışmanın asıl maksadı, risk yönetimi yaparak tespit edilecek risklerin ortadan kaldırılması/azaltılması değil, risk yönetiminin bazı adımlarından istifade ile riskleri, olasılık ve şiddetlerini tespit ederek ve bunu da çok kriterli karar verme yöntemine uyarlayarak farklı veri aktarım yöntemlerini veri linki güvenliği açısından karşılaştırmak ve sonucunda da önerdiğimiz yöntemin artı ve eksilerini ortaya koymaktır. Bu süreçte uygulanan İHA sistemleri için risk tabanlı çok kriterli karar verme modeli Şekil 6.2'de sunulmuştur. Çalışmada sadece İHA sistemlerinde bulunan kablosuz veri linkleri üzerinde durulmuş, GPS verisi ve kablolu linkler dahil edilmemiştir. Şekildeki mavi renk risk analizini, mor renk çok kriterli karar vermeyi, sarı renk ise ortak başlangıç ve bitiş noktalarını ifade etmektedir.

Bundan sonraki bölümde kullanılacak potansiyel tehlikelerin/kriterlerin, şiddet ve olasılıkların, alternatiflerin ve ağırlıkların belirlenebilmesi için geçmişte/halihazırda İHA ile ilgili bir birimde görev almış, İHA konusunda yetkin beş kişinin bilgi, tecrübe görüşlerinden istifade edilmiştir. Müteakip maddelerde, öncelikle yukarıda bahsedildiği ve modelde de görüldüğü üzere beş aşamalı risk yönetiminin ilk iki basamağı olan "Risk (tehlike) tanımlaması" ile "Risk değerlendirmesi (risk analizi)" uygulanacak, ardından çok kriterli karar verme modeline geçilecektir.



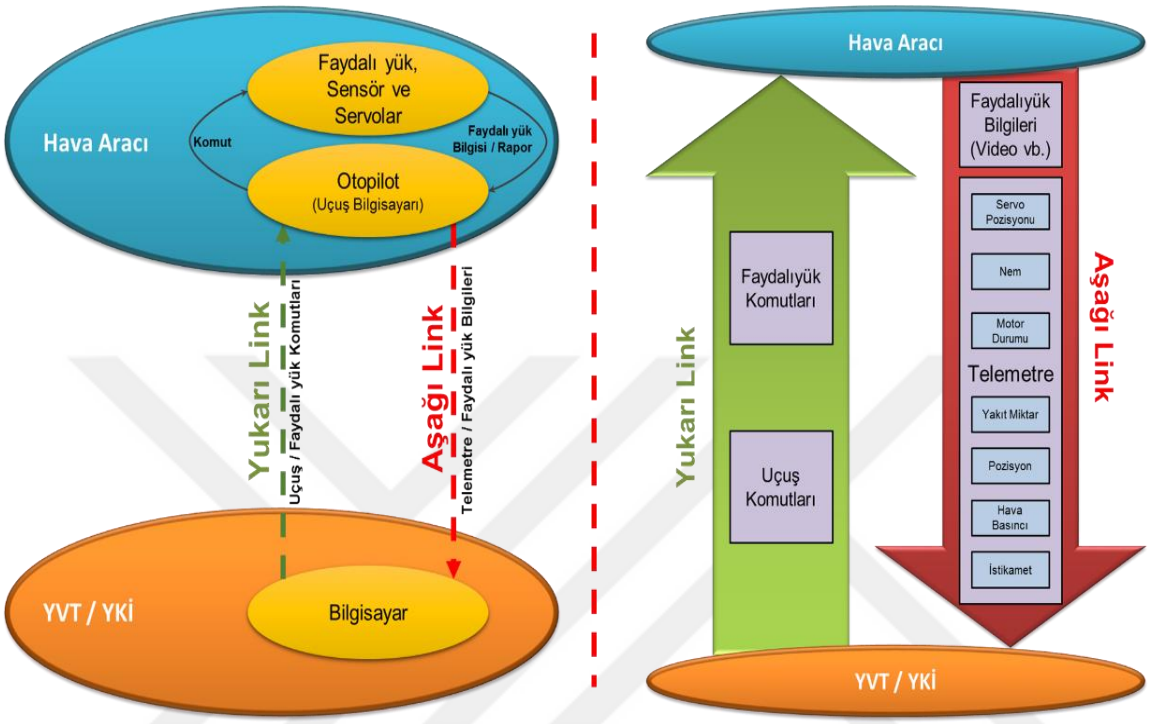
Şekil 6.2. İHA sistemleri için risk tabanlı çok kriterli karar verme modeli

6.3.1. Tehlikelerin belirlenmesi ve ön tehlike listesinin oluşturulması

İHA'larda risk analizi sürecinin amacı, İHA sisteminin nasıl başarısız olabileceğini, arızaların ve koşulların tehlikeler olarak nasıl ortaya çıkabileceğini ve tehlikelerin ortaya çıkmasından kaynaklanabilecek olası istenmeyen sonuçları belirlenmektir. Bu kapsamda risk analizi, tanımlanan risk senaryolarının her birinin doğasının ve seviyesinin karakterize edilmesi sürecini tanımlar [78]. Bahse konu süreçte ve tüm risk yönetiminde en önemli husus tehlikelerin doğru tespit edilebilmesidir. Bu maksatla, ayrıntıları üçüncü bölümde verilmiş olan İHA'larda veri linki (haberleşme) sistemi basit bir yaklaşımla incelenerek söz konusu tehlikeler belirlenecektir. Veri linklerinde esas olan, o linkte bulunan ve aktarılan verilerin güvenliğinin sağlanmasıdır. Bu maksatla şu soruların ve/veya benzerlerinin cevaplanması önem arz etmektedir:

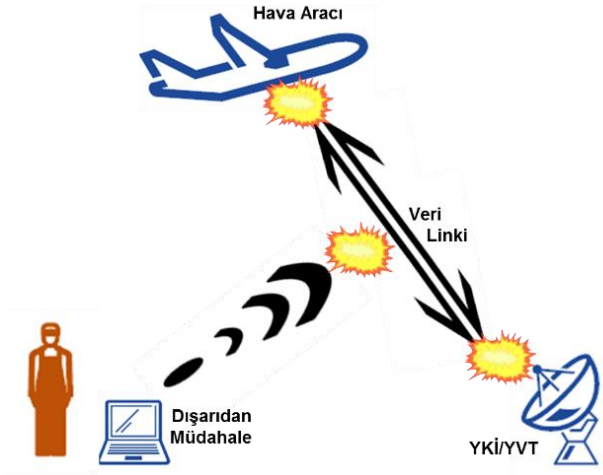
- Veriler nerede?
- Sistemde hangi veriler mevcut?
- Veriler nerede depolanıyor?
- Veriler hangi kanalla aktarılıyor?
- Veri nerelerde tehlikeye maruz kalabilir?
- Hangi tehlike sistemin hangi parçasını tehdit etmektedir?

İHA'dan/ya aktarılan veriler ile depolama/aktarma birimleri (veri akış şeması) Şekil 6.3'de görülmektedir. Bu şekilden, yukarıdaki soruların cevabını bulmak ve tehlikeleri tespit etmek için istifade edilmiştir.



Şekil 6.3. İHA'dan/ya aktarılan veriler ile depolama/aktarma birimleri (veri akış şeması)

Yukarıdaki şekil incelendiğinde verilere ilişkin zafiyetin esas olarak üç bölgede (İHA unsurunda) toplandığı değerlendirilmektedir. Bahse konu Potansiyel tehdit oluşturan İHA unsurları Şekil 6.4'de görülmektedir.



Şekil 6.4. Potansiyel tehdit oluşturan İHA unsurları

Yukardaki bilgiler ışığında, potansiyel ve/veya muhtemel tehlikeleri belirlemeye yönelik oluşturulmuş ve bir sonraki aşamada karar modelinin girdisi olacak kriterleri de içeren "Tehlike / Aksilik Çeklisti" Çizelge 6.1'de sunulmuştur.

Çizelge 6.1. Tehlike/aksilik çeklisti

1	İHA'ya saldırgan tarafından komut gönderilmesi
	1.1 Hedef bölgesinde kullanımının engellenmesi
	1.2 Farklı bölgeye yönlendirme
	1.3 Düşürme
	1.4 Belirlenen bir noktaya çarpma
	1.5 Başka bir hava/kara/deniz aracına çarpma
2	Faydalı yüke saldırgan tarafından komut gönderilmesi (faydalı yük tipine göre bu liste uzatılabilir)
	2.1 Uygun şekilde kullanımının engellenmesi
	2.2 Farklı noktanın lazer ile işaretlenmesi
	2.3 Güdümlü mühimmatın yanlış noktaya yönlendirilmesi
	2.4 İstenmeyen zamanda atış yapılması
	2.5 İstenmeyen noktaya atış yapılması
	2.6 İstenmeyen bölgenin görüntü ve resimlerinin alınması
3	İHA'nın koordinatlarının saldırgan tarafından belirlenmesi
	3.1 İHA hakkında hedef şahısların bilgilendirilmesi
	3.2 İHA'nın havada imha edilmesi
	3.3 İHA'ya elektronik harp uygulanarak bastırılması/karıştırılması
4	Faydalı yük verilerinin saldırgan tarafından alınması
5	Faydalı yükün işaret ettiği/baktığı noktanın koordinatlarının belirlenmesi
	5.1 Hedefteki şahısların ikaz edilmesi
	5.2 Görüntü ve resimlerin ele geçirilmesi
6	YKİ'ye saldırgan tarafından yanlış telemetre gönderilmesi
	6.1 Hava aracının yeri hakkında yanlış bilgi verilerek görevin engellenmesi
	6.2 Hava aracının yeri hakkında yanlış bilgi verilerek uçağın düşürülmesi
7	YKİ'ye saldırgan tarafından yanlış faydalı yük bilgisi gönderilmesi
	7.1 Faydalı yükün doğru/istenilen şekilde kullanımının engellenmesi
	7.2 Faydalı yükün istem dışı kullanımının sağlanması

Çizelge 6.1. (devam) Tehlike/aksilik çeklisti

8	Veri tabana saldırgan tarafından erişim sağlanması	
	8.1	Veri tabanındaki bilgilerin ele geçirilmesi
	8.2	Veri tabanın silinmesi
9	YKİ'nin saldırgan tarafından kullanım dışı bırakılması	
	9.1	Hava aracı kontrolünün ve görevin engellenmesi
	9.2	Hava aracı kontrolünün engellenmesi ve düşmesine neden olunması
10	Diğer tehlikeler	
	10.1	İnsan*: Uçuş ekibinin; yetersizlik, tecrübesizlik, bilgisizlik, yorgunluk, motivasyon düşüklüğü vb. nedenlerle oluşturduğu tehlikeler
	10.2	İnsan: Bölgede yeterli fiziki güvenlik tedbirlerinin alınmamasının oluşturacağı tehlikeler
	10.3	İnsan: Uçuş ekibi görevlendirmesinin uygun şekilde yapılmamasın oluşturacağı tehlikeler
	10.4	İnsan: Teknik bülten ve yazılımların güncel olmaması
	10.5	Makine*: Fiziki şartların uygun olmamasından kaynaklanabilecek tehlikeler
	10.6	Makine: Meteorolojik şartların sistem üzerine olumsuz etkileri
	10.7	Makine: Uçuş için hayati öneme sahip sistemlerin yedekli olmaması
	10.8	Çevre*: Sistem limitlerinin kesin olarak belirlenememesi
	10.9	Çevre: Prosedürlerin uygun olarak belirlenmemesi

* İnsan, makine ve çevre/ortam kazaya neden olan ana faktör gruplarıdır.

Tehlike miktarını artırmak ve çeklisti uzatmak her zaman mümkündür. Ancak burada listelenen tehlikeler veri linkine ilişkin olarak beş kişilik uzman ekip tarafından, yapılacak risk tabanlı karar verme modeline esas teşkil edecek şekilde belirlenmiştir. Tehlike/kriterlere ilişkin şiddet, olasılık ve ağırlıklar da benzer şekilde belirlenmiştir.

Tehlike Çeklisti oluşturularak belirlenen tehlikeler Çizelge 6.2'de sonraki aşamalarda kullanılmak üzere sadeleştirilerek listelenmiş ve birer kısaltma belirlenmiştir.

Çizelge 6.2. Tespit edilen tehlikeler ve kısaltmaları

Kısaltma	Tehlike
T1	Hedef bölgesinde kullanımının engellenmesi
T2	Farklı bölgeye yönlendirme
T3	Düşürme
T4	Belirlenen bir noktaya çarpma

Çizelge 6.2. (devam) Tespit edilen tehlikeler ve kısaltmaları

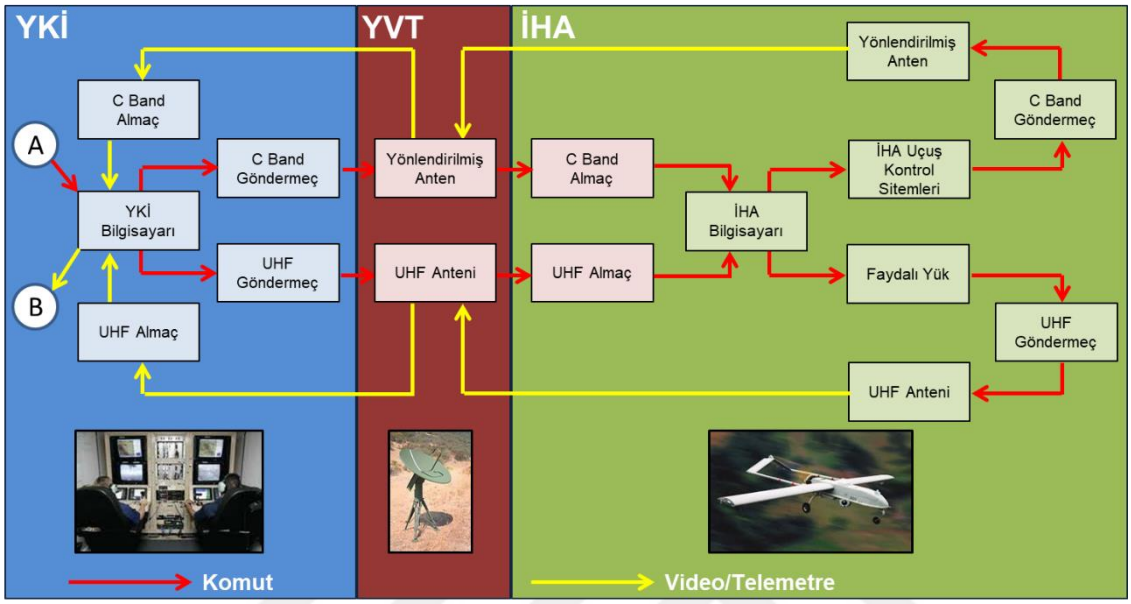
T5	Başka bir hava/kara/deniz aracına çarpma
T6	Uygun şekilde kullanımının engellenmesi
T7	Farklı noktanın lazer ile işaretlenmesi
T8	Güdümlü mühimmatın yanlış noktaya yönlendirilmesi
T9	İstenmeyen zamanda atış yapılması
T10	İstenmeyen noktaya atış yapılması
T11	İstenmeyen bölgenin görüntü ve resimlerinin alınması
T12	İHA hakkında hedef şahısların bilgilendirilmesi
T13	İHA'nın havada imha edilmesi
T14	İHA'ya elektronik harp uygulanarak bastırılması/karıştırılması
T15	Faydalı yük verilerinin saldırgan tarafından alınması
T16	Hedefteki şahısların ikaz edilmesi
T17	Görüntü ve resimlerin ele geçirilmesi
T18	Hava aracının yeri hakkında yanlış bilgi verilerek görevin engellenmesi
T19	Hava aracının yeri hakkında yanlış bilgi verilerek uçağın düşürülmesi
T20	Faydalı yükün doğru/istenilen şekilde kullanımının engellenmesi
T21	Faydalı yükün istem dışı kullanımının sağlanması
T22	Veri tabanındaki bilgilerin ele geçirilmesi
T23	Veri tabanın silinmesi
T24	Hava aracı kontrolünün ve görevin engellenmesi
T25	Hava aracı kontrolünün engellenmesi ve düşmesine neden olunması
T26	Uçuş ekibinin; yetersizlik, tecrübesizlik, bilgisizlik, yorgunluk, motivasyon düşüklüğü vb. nedenlerle oluşturduğu tehlikeler
T27	Bölgede yeterli fiziki güvenlik tedbirlerinin alınmamasının oluşturacağı tehlikeler
T28	Uçuş ekibi görevlendirmesinin uygun şekilde yapılmamasın oluşturacağı tehlikeler
T29	Teknik bülten ve yazılımların güncel olmaması
T30	Fiziki şartların uygun olmamasından kaynaklanabilecek tehlikeler
T31	Meteorolojik şartların sistem üzerine olumsuz etkileri
T32	Uçuş için hayati öneme sahip sistemlerin yedekli olmaması
T33	Sistem limitlerinin kesin olarak belirlenememesi
T34	Prosedürlerin uygun olarak belirlenmemesi

6.3.2. Ön tehlike analizinin yapılması ve risk değerlendirmesi

Ön tehlike analizinde, ön tehlike listesi metodunda tespit edilemeyen tehlikeleri de tespit etme imkanı bulunmaktadır. Bu maksatla "Güvenlik Blok Diyagramları" ve "Fonksiyonel Blok Diyagramları" yaygın olarak kullanılmaktadır. İHA'larda veri linkine ilişkin hazırlanmış güvenlik blok diyagramı Şekil 6.5'de görülmektedir.

Veri linki güvenlik diyagramında da istifade ile ön tehlike analizinde ve öncesinde ön tehlike listesi çalışmasında belirlenen tehlike listesinin risk analizlerinin yapılabilmesi için öncelikle

belirlenen tehlikelere yönelik olasılık ve şiddet tespit edilmekte, sonucunda da risk değerlendirme matrisi oluşturulmakta, bu verilerden de "Ön Tehlike Analiz Formunda" istifade edilmektedir.



Şekil 6.5. Veri linkine ilişkin hazırlanmış güvenlik blok diyagramı

İHA güvenlik risk olasılığı

Güvenlik riski olasılığı, bir güvenlik tehlikesinin sonucu veya sonucunun ortaya çıkma ihtimali veya sıklığı olarak tanımlanır. Bu süreçte; tüm senaryolar dikkate alınmalı, olasılık belirli kriterlere göre sınıflandırılmalı ve seviyelendirilmelidir. Çalışmada kullandığımız risk olasılıkları Çizelge 6.3'de sunulmuştur. Olasılık sınıfları genel olarak harflerle (A, B, C, vb.) ifade edilmesine rağmen risk tabanlı çok kriterli karar verme modelinde ağırlıkları oluşturacağından 1-5 seviyelerinde sayısal olarak verilmiştir.

Çizelge 6.3. Risk olasılıkları

Olasılık	Seviye	Spesifik Olay
Sık	5	Sık sık meydana gelebilir.
Muhtemel	4	Sistem hayatı boyunca sık olmayacak şekilde defalarca ortaya çıkabilir.
Ara Sıra	3	Sistem hayatı boyunca uzun aralıklarla oluşabilir.
Uzak	2	Ortaya çıkma olasılığı göz ardı edilemez.
İhtimal dışı	1	Olasılığı sıfıra yakın olduğundan göz ardı edilebilir.

İHA güvenlik risk şiddeti

Güvenlik riski, belirlenmiş tehlikelerin bir sonucu veya sonucu olarak ortaya çıkabilecek zararın derecesi olarak tanımlanır. Ciddiyet değerlendirmesi, yaralanmalara (kişilere) ve/veya hasarlara (İHA'nın kendisi, binalar, elektrik hatları vs. / maliyet boyutu) dayanabilir. Tespitler yapılırken; en kötü öngörülebilir durum hesaba katılmalı, şiddet belirli kriterlere göre sınıflandırılmalı ve seviyelendirilmelidir. İHA veri linki güvenliği için oluşturulmuş risk şiddetleri Çizelge 6.4'dedir.

Çizelge 6.4. Risk şiddetleri

Şiddet	Seviye	Spesifik Olay
Hayati	5	Külli kırım.
Büyük	4	Kısmi kırım.
Marjinal	3	Çok sayıda parça değişimi ile giderilebilen hasar.
Hafif	2	Onarılabilen hasar.
Önemsiz	1	Uçuşu etkilemeyen hasar.

İHA güvenlik risk değerlendirme matrisi

İHA güvenlik risk olasılık ve şiddetlerinin belirlenmesini müteakip eşitlik Eş. 6.1 ile İHA güvenlik risk değerlendirme matrisi oluşturulmuştur. Bu eşitlikte risk (R), olasılık (O) ve şiddetin (S) çarpımı olarak ifade edilmiştir.

$$R_i = O_i \, x \, S_i \tag{6.1}$$

Bu matris önceden belirlenmiş olasılık ve şiddetlere göre tehlikelerin risklerini belirlemekte ve riskleri önem derecesine göre sınıflandırmaktadır [79]. İHA veri linkine ilişkin risk değerlendirme matrisi Çizelge 6.5'de görülmektedir. Kırmızı "korkunç risk", mavi "yüksek risk", sarı "orta risk", yeşil ise "düşük risk"i olan tehlikeleri ve değerlerini göstermektedir.

Uzman heyet tarafından her tehlike için değerlendirilen şiddet ve olasılık ile Eş. 6.1 çerçevesinde belirlenen risk ve ortalama riskler Çizelge 6.6'da sunulmuştur.

Çizelge 6.5. Risk değerlendirme matrisi

		Olasılık				
		Sık	Muhtemel	Ara Sıra	Uzak	İhtimal Dışı
Şiddet	Hayati	5x5=25	5x4=20	5x3=15	5x2=10	5x1=5
	Büyük	4x5=20	4x4=16	4x3=12	4x2=8	4x1=4
	Marjinal	3x5=15	3x4=12	3x3=9	3x2=6	3x1=3
	Hafif	2x5=10	2x4=8	2x3=6	2x2=4	2x1=2
	Önemsiz	1x5=5	1x4=4	1x3=3	1x2=2	1x1=1

Çizelge 6.6. Uzman heyet tarafından değerlendirilen şiddet, olasılık ve riskler

Kriter	Uzman 1			Uzman 2			Uzman 3			Uzman 4			Uzman 5			Ortalama Risk
	Ş	O	R	Ş	O	R	Ş	O	R	Ş	O	R	Ş	O	R	
T1	3	2	6	2	3	6	2	2	4	3	2	6	4	2	8	6
T2	4	2	8	4	2	8	2	2	4	4	2	8	3	4	12	8
T3	5	2	10	4	3	12	5	1	5	2	4	8	5	3	15	10
T4	5	2	10	5	2	10	4	2	8	5	2	10	4	3	12	10
T5	5	2	10	5	2	10	3	4	12	4	2	8	5	2	10	10
T6	3	3	9	3	4	12	4	2	8	2	2	4	4	3	12	9
T7	4	2	8	5	2	10	2	2	4	4	3	12	3	2	6	8
T8	5	2	10	4	2	8	4	3	12	5	1	5	5	3	15	10
T9	4	3	12	5	2	10	4	2	8	5	2	10	5	4	20	12
T10	4	2	8	2	2	4	3	2	6	5	2	10	4	3	12	8
T11	2	3	6	3	2	6	2	3	6	4	2	8	2	2	4	6
T12	3	4	12	5	2	10	4	4	16	4	3	12	5	2	10	12
T13	5	3	15	5	3	15	5	3	15	5	4	20	5	2	10	15
T14	4	5	20	5	5	25	5	5	25	4	5	20	5	2	10	20
T15	3	3	9	4	3	12	4	2	8	5	2	10	3	2	6	9
T16	2	2	4	3	1	3	2	2	4	3	2	6	3	1	3	4
T17	1	3	3	3	1	3	2	2	4	2	1	2	3	1	3	3
T18	2	3	6	3	2	6	4	2	8	2	3	6	2	2	4	6
T19	5	2	10	5	2	10	5	2	10	4	3	12	4	2	8	10
T20	3	2	6	2	2	4	4	2	8	2	2	4	4	2	8	6
T21	3	2	6	4	2	8	2	3	6	2	2	4	2	3	6	6
T22	3	4	12	5	2	10	5	3	15	4	2	8	5	3	15	12
T23	3	3	9	4	2	8	5	2	10	3	4	12	3	2	6	9
T24	4	4	16	4	5	20	4	3	12	4	3	12	5	4	20	16
T25	5	4	20	5	2	10	5	5	25	5	5	25	4	5	20	20
T26	4	3	12	3	4	12	3	4	12	4	4	16	4	2	8	12
T27	3	2	6	3	2	6	4	2	8	2	3	6	2	2	4	6
T28	2	3	6	4	2	8	3	2	6	2	2	4	3	2	6	6
T29	2	4	8	3	2	6	4	3	12	4	2	8	2	3	6	8
T30	3	3	9	5	2	10	3	2	6	4	2	8	3	4	12	9
T31	2	4	8	4	2	8	2	4	8	5	2	10	3	2	6	8
T32	5	2	10	3	4	12	4	2	8	4	2	8	4	3	12	10
T33	4	2	8	3	2	6	4	2	8	3	4	12	3	2	6	8
T34	4	2	8	4	2	8	5	1	5	5	2	10	3	3	9	8

Belirlenen risk olasılıkları, şiddetleri ve risk değerlendirme matrisi kapsamında önceden tespit edilmiş olan tüm tehlikelerin risk durumları değerlendirilmiş ve sonuçları Çizelge 6.7'de sunulan risk analiz tablosunda verilmiştir.

Çizelge 6.7. Risk analiz tablosu

Risk Seviyesi	Tehlikeler	Risk Aralığı
Korkunç Risk	T14, T25	25-20
Yüksek Risk	T13, T24	15-16
Orta Risk	T2-10, T12, T15, T19, T22-23, T26, T29-34	12-8
Düşük Risk	T1, T11, T16-18, T20-21, T27-28	6-1

Risk analizi neticesinde korkunç risk grubunda olan iki ve yüksek risk grubunda olan iki tehlike tespit edilmiştir. Bu tehlikeler risk büyüklüğü açından sırası ile şunlardır:

- T14 İHA'ya elektronik harp uygulanarak bastırılması/karıştırılması,
- T25 Hava aracı kontrolünün engellenmesi ve düşmesine neden olunması,
- T24 Hava aracı kontrolünün ve görevin engellenmesi,
- T13 İHA'nın havada imha edilmesi.

6.3.3. Risk tabanlı çok kriterli karar verme ile yöntemlerin karşılaştırılması

Risk tabanlı çok kriterli karar verme ile; risk analizinden elden edilen tehlikeler kriter olarak, olasılık ve şiddet çarpımı olan riskler ise ağırlık olarak kullanılarak önerdiğimiz yöntem de dahil literatür taramasından uzman heyetçe belirlenen alternatifler karşılaştırılacaktır.

Alternatiflerin belirlenmesi sürecinde literatür taramasında elde edilen önemli uygulama önerileri aşağıda çıkarılmıştır.

- İHA üzerinde bulunan CPU ile verilerin şifrelenmesini,
- İHA'larda veri transferi güvenliğinin sağlanmasına yönelik çok kademeli dinamik anahtar yönetim sistemi geliştirilmesi,
- Sıkıştırılmış video verileri için video şifreleme algoritması kullanılması,
- İHA üzerindeki kameranın görüntüsünün Rijndael algoritması ile şifrelenmesini müteakip gönderilmesi,

- On-board şifreleme, donanımsal şifreleme ve uygulama katmanı şifreleme alternatiflerinin kullanılması,
- Bir sertifika ile korunan veri linki ve kullanıcı yönetim sistemi geliştirilmesi,
- Eliptik eğriler yönteminin kullanılması.

Bu önerilerin içinde bizim çalışmamıza ana hatları ile en yakın olan Alex Wilson'ın önerisidir [12]. Wilson, veri linkini, hava aracı, komut ve faydalı yük olarak üç grupta incelemiş, çok kademeli ve uçtan uca güvenli bir sistem kurulması gerektiğini ileri sürmüş, bu maksatla; kullanıcı yönetim sistemi geliştirilmesi gerektiğini de açıklamıştır. Literatür taramasından elde edilen öneriler incelendiği, risk tabanlı çok kriterli karar verme modeli için ana hatları ile beş alternatif yöntem belirlenmiştir:

- A1 Açık gönderme,
- A2 Yazılımsal şifreleme,
- A3 Donanımsal şifreleme,
- A4 Kanal şifreleme,
- A5 Önerilen güvenli görüntü aktarım metodu.

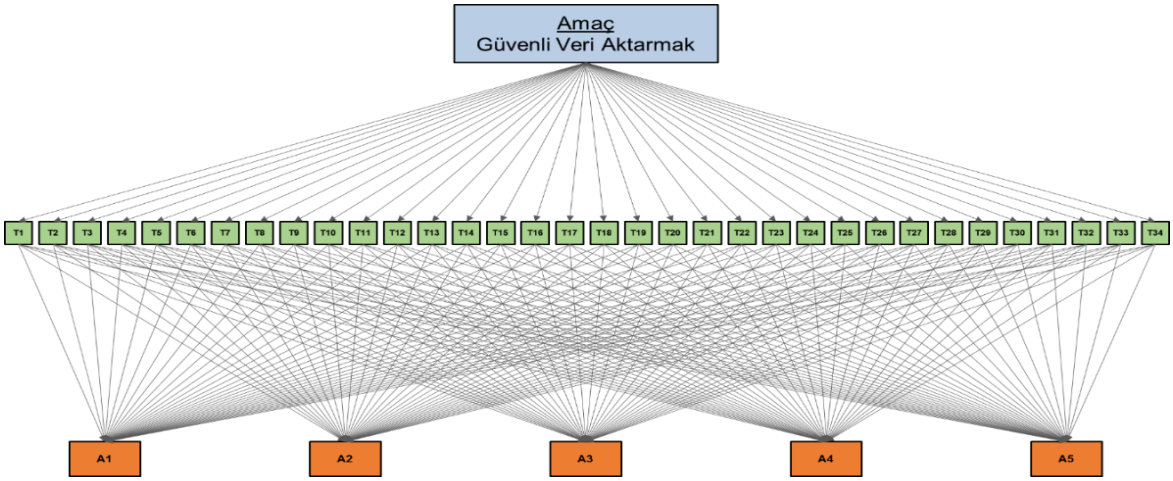
Risk tabanlı çok kriterli karar verme modeli, çalışmanın veri güvenliği odaklı olması ve isminden de anlaşılacağı üzere risklere dayalı olması nedeni ile yöntemlerin maliyet, ağırlık, kullanım kolaylığı vb. kriterler açısından karşılaştırılması karar matrisine yansıtılmayacaktır. Bu bakış açısıyla;

- Verilerin (telemetre, video, vb.) ayrı olarak yazılımsal olarak şifrelenmesinin İHA üstündeki kısıtlı CPU ve güç ile yapılmasının, tüm verilerin şifrelenmesinde ihtiyaç duyulan süreyi uzatacağı, dolayısı ile görüntü aktarımının gerçek zamanlı yapılamayacağı,
- Donanımsal şifreleme için hem hava aracında hem de YKİ'de ilave donanıma ihtiyaç duyulacağı, bunun da İHA'ya ilave ağırlık ve güç kaynağı yükü getireceği ve İHA sisteminin tasarımdan itibaren gözden geçirilmesini gerektireceği göz önünde bulundurulmalıdır.

Yukarıda ayrıntılarıyla anlatılmış olan güvenli görüntü aktarım metodun özellikle güvenlik ve güvenilirlik açısından getirdiği avantajlar aşağıda sunulmuştur.

- Motion-JPEG kullanılması:
  - Düşük işlemci ve bellek gereksinimi,
  - Video akışında meydana gelen hızlı değişimleri kolayca tolere edebilmesi,
  - Yazılımda yapılan geliştirme ile daha az ve hızlı görüntü aktarımı.
- TCP kullanılması:
  - Bağlantı odaklı olması,
  - Verilerin bozulmadan ve gönderildiği sırayla gideceği garantisi,
  - Üç yönlü el sıkışma ile akış kontrolü ve hata kontrolü/düzeltmesi yapılması.
- TLS protokolünün kullanılması:
  - Sertifika ve anahtara dayalı şifreli kanal oluşturması,
  - İki yönlü veri aktarımı yapılabilmesi,
  - Hem telemetre (komut ve rapor) hem de video gibi verilerin eş zamanlı olarak gönderilebilmesi,
  - Hava aracı üzerinde ilave donanım ihtiyacı gerektirmemesi.
- Kullanıcı giriş sistemi oluşturulması:
  - Kullanıcı adı ve şifre karşılaştırma ve doğrulama gerektirmesi,
  - Bağlantı talep eden IP ile yetkilendirilen IP'lerin karşılaştırılması,
  - Bağlantı talep eden unsurun koordinatları ile YKİ'nin bilinen koordinatlarının karşılaştırılması.

Bu hususlardan, risk tabanlı çok kriterli karar verme aşamasında istifade edilmiştir. Karar verme sürecinde, basitliği ve amaca uygunluğu nedeni ile Ağırlıklı Toplam Yöntemi çok kriterli karar verme modeli olarak belirlenmiş, hem tecrübe ve bilgiden hem de sayısal olgu ve verilerden istifade edilmek esas alındığından kalitatif ve kantitatif karışımı hibrit bir yaklaşım tercih edilmiştir. Karar matrisi oluşturulurken sayısal ağırlık ve oranlardan istifade edilmiş ancak bu ağırlık ve oranlar uzman grubun bilgi ve tecrübelerine dayalı olarak tespit edilmiştir. Ağırlıklı karar matrisi oluşturulurken kolaylık sağlaması açısından Şekil 6.6'da görülen karar modeli hiyerarşik yapısı hazırlanmıştır.



Şekil 6.6. Karar modeli hiyerarşik yapısı [80]

Risk tabanlı çok kriterli karar vermenin son aşamasında, yukardaki tüm veriler kullanılarak ağırlıklı karar matrisi oluşturulmuştur. Ağırlıklar (w) doğrudan risk analizinden alınarak toplamı "1" olacak şekilde Eş. 6.2'ye göre ölçeklendirilmiş ve Eş. 6.3'e göre hesaplanmıştır.

$$\sum_{i=1}^{34} w_i = 1 \tag{6.2}$$

$$w_i = \frac{R_i}{\sum_{j=1}^{34} R_j} = \frac{O_i S_i}{\sum_{j=1}^{34} O_j S_j} \tag{6.3}$$

$$w_{17} = \frac{3}{320} = 0{,}009$$

$$w_{16} = \frac{4}{320} = 0{,}013$$

$$w_1 = w_{11} = w_{18} = w_{20} = w_{21} = w_{27} = w_{28} = \frac{6}{320} = 0{,}019$$

$$w_2 = w_7 = w_{10} = w_{29} = w_{31} = w_{33} = w_{34} = \frac{8}{320} = 0{,}025$$

$$w_6 = w_{15} = w_{23} = w_{30} = \frac{9}{320} = 0{,}028$$

$$w_3 = w_4 = w_5 = w_8 = w_{19} = w_{32} = \frac{10}{320} = 0{,}031$$

$$w_9 = w_{12} = w_{22} = w_{26} = \frac{12}{320} = 0{,}038$$

$$w_{13} = \frac{15}{320} = 0{,}047$$

$$w_{24} = \frac{16}{320} = 0{,}050$$

$$w_{14} = w_{25} = \frac{20}{320} = 0{,}063$$

Bu hesaplamalar kapsamında hazırlanan ağırlıklı karar matrisi Çizelge 6.8'de sunulmuştur.

Çizelge 6.8. Ağırlıklı karar matrisi

Alternatif			A1		A2		A3		A4		A5	
Kriter	Risk	Ağırlık	KKO	Değer	KKO	Değer	KKO	Değer	KKO	Değer	KKO	Değer
T1	6	0,019	1	0,019	1	0,019	1	0,019	2	0,038	5	0,094
T2	8	0,025	1	0,025	3	0,075	3	0,075	5	0,125	5	0,125
T3	10	0,031	1	0,031	3	0,094	3	0,094	5	0,156	5	0,156
T4	10	0,031	1	0,031	4	0,125	4	0,125	5	0,156	5	0,156
T5	10	0,031	1	0,031	4	0,125	4	0,125	5	0,156	5	0,156
T6	9	0,028	1	0,028	2	0,056	2	0,056	3	0,084	3	0,084
T7	8	0,025	1	0,025	3	0,075	3	0,075	5	0,125	5	0,125
T8	10	0,031	1	0,031	4	0,125	4	0,125	5	0,156	5	0,156
T9	12	0,038	1	0,038	3	0,113	3	0,113	5	0,188	5	0,188
T10	8	0,025	1	0,025	4	0,100	4	0,100	5	0,125	5	0,125
T11	6	0,019	1	0,019	3	0,056	3	0,056	5	0,094	5	0,094
T12	12	0,038	1	0,038	2	0,075	2	0,075	4	0,150	5	0,188
T13	15	0,047	1	0,047	2	0,094	2	0,094	5	0,234	5	0,234
T14	20	0,063	1	0,063	1	0,063	1	0,063	1	0,063	1	0,063
T15	9	0,028	1	0,028	3	0,084	3	0,084	4	0,113	5	0,141
T16	4	0,013	1	0,013	3	0,038	3	0,038	4	0,050	5	0,063
T17	3	0,009	1	0,009	2	0,019	2	0,019	3	0,028	4	0,038
T18	6	0,019	1	0,019	3	0,056	3	0,056	4	0,075	5	0,094
T19	10	0,031	1	0,031	4	0,125	4	0,125	5	0,156	5	0,156
T20	6	0,019	1	0,019	3	0,056	3	0,056	4	0,075	4	0,075
T21	6	0,019	1	0,019	3	0,056	3	0,056	4	0,075	5	0,094
T22	12	0,038	1	0,038	2	0,075	2	0,075	3	0,113	4	0,150
T23	9	0,028	1	0,028	2	0,056	2	0,056	3	0,084	3	0,084
T24	16	0,050	1	0,050	3	0,150	3	0,150	4	0,200	4	0,200
T25	20	0,063	1	0,063	3	0,188	3	0,188	5	0,313	5	0,313
T26	12	0,038	1	0,038	2	0,075	2	0,075	2	0,075	3	0,113
T27	6	0,019	1	0,019	2	0,038	2	0,038	2	0,038	2	0,038
T28	6	0,019	1	0,019	2	0,038	2	0,038	2	0,038	3	0,056
T29	8	0,025	1	0,025	2	0,050	2	0,050	2	0,050	2	0,050
T30	9	0,028	1	0,028	2	0,056	2	0,056	2	0,056	3	0,084
T31	8	0,025	1	0,025	1	0,025	1	0,025	1	0,025	1	0,025
T32	10	0,031	1	0,031	1	0,031	1	0,031	1	0,031	1	0,031
T33	8	0,025	1	0,025	1	0,025	1	0,025	1	0,025	1	0,025
T34	8	0,025	1	0,025	1	0,025	1	0,025	1	0,025	1	0,025
Toplam Değer (1-5)		1,000	1,000		2,459		2,459		3,494		3,797	

Matriste, karara niceliksel olarak ulaşabilmek adına alternatiflerin her bir kriteri ne oranda karşıladığını belirlemek için "Kriter karşılama oranı (KKO)" kullanılmıştır. KKO'lar, uzman heyetin 1-5 aralığında verdiği değerlerin ortalaması alınarak belirlenmiştir. Ağırlıklarda büyüklük risk artışını gösterdiğinden, alternatifin kriteri tamamen karşılama

durumu 5, karşılamama durumu ise 1 ile ifade edilmiştir. Her bir kriter için ağırlık ve KKO çarpımı da "Değer (D)" olarak isimlendirilmiştir. Değerin yüksek olması, o alternatifin önemli bir kriteri yüksek oranda karşılaması anlamına gelirken, değerin düşük olması o alternatifin daha az önemli bir kriteri daha düşük oranda karşılaması ya da hiç karşılamaması anlamına gelmektedir. Bu bilgiler ve hesaplamalar kapsamında risk tabanlı çok kriterli karar verme modeli aslında Eş. 6.4'de bulunan matematik modele dayalı bir optimizasyon problemi halini almıştır.

$$Max\ Total\ Value = \sum_{i=1}^{34} D_i$$

$$= \sum_{i=1}^{34} KKO_i \times w_i$$

$$= \sum_{i=1}^{34} (KKO_i \times \frac{R_i}{\sum_{j=1}^{34} R_j})$$

$$= \sum_{i=1}^{34} (KKO_i \times \frac{O_i S_i}{\sum_{j=1}^{34} O_j S_j}) \quad (6.4)$$

Ağırlıklı karar matrisinin sonucu incelendiğinde;

- A1-Açık gönderme yönteminin zaten beklendiği üzere veri linki güvenliği açısından en zayıf yöntem olduğu,
- A2-Yazılımsal şifreleme ile A3-Donanımsal şifreleme alternatiflerinin aynı derecede ve tüm yöntemler göz önünde bulundurulduğunda ortalama seviyede güvenlik sağladığı,
- A4-Kanal şifreleme yönteminin ilk üç alternatife kıyasla iyi seviyede veri linki güvenliği sağladığı,
- Ancak A5-Önerilen güvenli görüntü aktarım metodunun, A4-Kanal şifrelemeye kıyasla veri linki güvenliğinde yaklaşık % 8,7 iyileştirme sağladığı görülmektedir.

Ayrıca önceden de açıklandığı gibi; çalışmanın veri güvenliği odaklı ve risklere dayalı olması nedeni ile alternatiflerin maliyet, ağırlık, kullanım kolaylığı vb. kriterler açısından değerlendirilmediği göz önünde bulundurulduğunda önerilen yöntemin tercih edilme oranının daha da artacağı değerlendirilmektedir.

7. SONUÇ VE ÖNERİLER

İHA'ların yaygınlaşması ile kullanım alanları ve güvenlikleri ile güvenilirlikleri sorgulanır hale gelmiştir. İHA'ların hala en yaygın kullanım maksadının keşif ve gözetleme olduğu ve İHA sistemlerindeki verinin önemi göz önünde bulundurulduğunda İHA sistemlerinin en kritik alt sisteminin haberleşme (veri linki) olduğu açıkça görülmektedir. Bu nedenle; veri linkine dışardan müdahalenin önlenmesi ve uzun mesafelerde veri iletiminde doğru bilginin doğru noktaya gönderilebilmesi maksadıyla güvenli görüntü/veri aktarım yönteminin geliştirilmesi hedef alınmıştır.

Çalışmaya temel oluşturması ve konunun tüm yönüyle ortaya konulabilmesi için İHA'nın tanımı ve tarihçesi ile birlikte kullanım alanları, tasnifi ve unsurlarından araştırılmıştır. Üzerinde inceleme yapabilmek adına 3 boyutlu bir İHA modeli oluşturulmuş ve bu model üzerinde Sonlu Elemanlar Metoduyla akış analizi yapılmış, neticesinde; "İnsansız Bir Hava Aracı Modelinin Üç Boyutlu Tasarımı, Analizi ve Simülasyonu" konulu makale, 11-12 Kasım 2015 tarihlerinde ODTÜ'de gerçekleştirilen "6. Ulusal Savunma Uygulamaları Modelleme ve Simülasyon Konferansı (USMOS 2015)"de sunulmuştur.

İkinci aşamada, İHA'ların haberleşmesi sistemleri ile komuta mantığı incelenmiş, haberleşme alt sistemi, frekans planlama ve tahsis kriterleri araştırılmış; haberleşmenin daha net anlaşılabilmesi için genel olarak radyo frekans haberleşme ve sinyal istikameti bulma yöntemlerine incelenmiştir. Bu bölümde edinilen bilgiler ile hazırladığımız "Unmanned Air Vehicle System's Data Links" konulu makale, 27-28 Nisan 2015 tarihlerinde Gazi Üniversitesi'nde gerçekleştirilen "2nd International Conference on Electrical and Electronics Engineering (ICEEE 2016)"de arz edilmiş ve Journal of Automation and Control Engineering'de yayımlanmıştır.

İHA veri linkinin güvenliğinin nasıl sağlanacağını ortaya koyabilmek için İHA'lara karşı yapılabilecek saldırı türleri incelenmiş, yaygın olarak kullanılan saldırı yöntemleri ortaya konmuş ve örnek tespit/saldırı olaylarına değinilmiştir. Bu süreçte, önceden edinilmiş tecrübeye dayalı ve "The Aspects, Reasons and Outcomes of an Unmanned Air Vehicle Crash Caused By Engine Failure" konulu makale, 20-23 Mayıs 2015 tarihlerinde Kore'de gerçekleştirilen "8th Asian-Pacific Conference on Aerospace Technology and Science

(APCATS 2015)"de arz edilmiş ve International Journal of Aerospace System Engineering'de yayımlanmıştır.

Bir yöntem geliştirmeden önce son olarak, verilerin depolanma ve aktarılma esnasında güvenliğinin sağlanabilmesi için yöntem geliştirme yolunda kriptografinin ne olduğu ne hangi yöntemlerle verilerin şifrelenebileceği araştırılmıştır. Şifreleme için kullanılacak karmaşık algoritmaları sorunu ve gecikmeyi artırdığından, gömülü video sistemi ve hava aracı sınırlı bataryayı paylaşmak zorunda olduğundan ve büyük video verisi ve sınırlı kaynaklar arasında ciddi uyumsuzluk oluşturduğundan şifreleme düzeninin mümkün olduğunca basit tasarlanması gerektiği sonucuna ulaşılmıştır.

İHA'larda kullanılmakta olan güvenli veri aktarım ve kriptolama yöntemleri ile örnek ele geçirme olayları araştırılarak, güvenli bir veri aktarım yöntemi geliştirilmeye çalışılmıştır. Bu maksatla Raspberry Pi 3 ve kamerasına dayalı bir geliştirme ortamı hazırlanmıştır. Bu ortamda, yazılan kod ile HTTP üzerinden Motion-JPEG görüntü aktarımı sağlanmış ve bu maksatla TCP/IP protokol yapısı ile TLS protokollerinde istifade edilerek veri aktarımı için şifreli bir kanal oluşturulmuş ve verilerin kriptolu aktarımı yapılmıştır.

Dijital kameralar, IP kameralar ve web kameraları gibi video yakalama cihazları tarafından yaygın olarak kullanılması, video akışında meydana gelen hızlı değişimleri kolayca tolere edebilmesi, Safari, Google Chrome, Mozilla Firefox ve Microsoft Edge gibi web tarayıcılar tarafından desteklenmesi, video akışında meydana gelen hızlı değişimleri kolayca tolere edebilmesi ve minimum donanım ihtiyacı nedenleri ile Motion-JPEG formatının kullanılmasını tercih edilmiştir.

HTTP desteği, bağlantı odaklı olması, yüksek güvenilirlik gerektiren uygulamalar için uygun olması, verilerin bozulmadan ve gönderildiği sırayla gideceği garantisi, üç yönlü el sıkışma ile Akış Kontrolü ve Hata Kontrolü/Düzeltme yapması gibi avantajlara sahip olması nedeniyle de IP trafiği olarak TCP kullanılmıştır. Sertifika ve anahtara dayalı şifreli kanal oluşturduğu, daha çok veriyi daha kısa sürede şifreleyerek aktarabildiği, bu maksatla hava aracı üzerinde ilave donanım ihtiyacı gerektirmediği, aynı zamanda iki yönlü veri akışı güvenli olarak sağlayabildiği, hem telemetre (komut ve rapor) hem de video gibi veriler eş zamanlı olarak gönderilebildiği için TLS protokolünün kullanılması tercih edilmiştir.

Yazılımda yapılan bir geliştirme ile görüntü aktarımı etkinleştirilmiş ve hızlandırılmıştır. Bu kapsamında; aynı resmin birden fazla gönderilmesi engellenmiş, böylece aktarılan resim sayısı ve paralelinde veri trafiği de benzer şekilde azaltılmış, aktarılan görüntünün netliği ve keskinliği artırılmış, CPU kullanımı ve paralelinde ihtiyaç duyulan donanım özelikleri düşürülmüş, kablosuz ağın kapasitesine bağlı olarak görüntü aktarımından istifade edebilecek istemci bağlantı sayısı artırılmıştır.

Şifreli kanala giriş ve çıkışlarında güvenli olması için bir arayüz ile kullanıcı giriş sistemi oluşturulmuştur. Kullanıcıların tüm bağlantıları kayıt altına alınmaktadır. Kullanıcı adı ve şifresinin güvenli kanal (TLS) üzerinden şifrelenerek gönderilmesi, böylece istenmeyen kişilerce (eavesdropping) elde edilememesi amaçlanmıştır. Sisteme giriş yapabilmek için; kullanıcı adı ve şifre karşılaştırma ve doğrulama, bağlantı talep eden IP ile yetkilendirilen IP'lerin karşılaştırma, yine bağlantı talep eden unsurun koordinatları ile YKİ'nin bilinen koordinatları karşılaştırma işlemleri yapılabilecektir.

Özünde, giriş sırasında dinleme (wiretapping) ve paket koklama (packet sniffing) saldırılarına karşı koruma sağlamak maksadıyla HTTPS protokolü kullanılmıştır. Hâlihazırda veriler, oluşturulan bu güvenli kanal ile aktarılırken bir de üzerine kullanıcıya özel filigran uygulaması çalışmasına devam edilmektedir. Böylelikle resim veya görüntünün sızdırılması durumunda açığın tespit edilmesinin kolaylaştırılması hedeflenmiştir.

Çalışmamızda, İHA sistemlerinde veri linki güvenliği sorununa bir çözüm bulmak için İHA ve yer kontrol istasyonu arasında karşılıklı olarak görüntülerin ve verilerin güvenli bir şekilde aktarılmasını sağlayacak bir yöntem üzerinde durulmuştur. Güvenli görüntü aktarımı için yeni bir şifreleme yöntemi geliştirilmemiş ancak var olan farklı yöntemler farklı bir alan olan İHA sistemlerine uyarlanarak ve birlikte kullanılarak alternatif bir yöntem geliştirilmiştir. Bu yolla, Motion-Jpeg, TCP/IP, TLS/SSL ve kullanıcı kimlik doğrulama/yetkilendirme sistemi ile dört adımlı bir güvenlik sistemi önerilmiştir. Sonuç olarak, bu düşük maliyetli, güvenilir, yönetilebilir, güvenli ve uygulanabilir yöntemde, veriler Raspberry Pi 3 ve Picamera modülü kullanılarak Go Language ile yazılan kod vasıtası ile HTTPS üzerinden aktarılmış ve yöntem ayrıca deneyle de doğrulanmıştır.

Çalışmanın son bölümünde ise Risk Yönetimi ve Karar Verme yöntemlerine kısaca değinilerek, önerilen güvenli görüntü aktarım yönteminin İHA uçuş güvenliğine katkısı ve

literatür taramasında tespit edilen diğer yöntemlerle risk tabanlı çok kriterli karar verme metodu ile karşılaştırma sonuçları ortaya konulmuştur. İHA sistemlerinin yaygın kullanımı ve önemi göz önünde bulundurulduğunda, karşılaşılabilecek tehlikelerin ve risklerin önceden belirlenmesi ve bu sistemlerin daha da güvenli hale getirilmesi için risk analizinden de faydalanılması gerektiği açıkça görülmektedir. İHA sistemini bir bütün olarak risk analizine tabi tutan çeşitli çalışmalar literatürde bulunmaktadır. Ancak İHA veri linkine ilişkin risk analizine yönelik bir çalışma tespit edilememiş ve ilk defa tarafımızca yapılmıştır. Çalışmamızın son bölümünde İHA veri linkine ilişkin risk analizini esas alacak şekilde, kendi önerdiğimiz güvenli görüntü aktarım metodu ile literatür taramasında tespit edilen toplam beş yöntemi karşılaştırarak değerlendirmeye tabi tutacak bir yöntem üzerinde durulmuştur. Karşılaştırma ve karar verme için uygun yöntem olarak Çok Kriterli Karar Verme Yöntemi temel alınmış ancak özgün bir yaklaşım olarak kriterlerin belirlenmesi ve alternatiflerin karşılaştırılmasında Risk Analizi metodolojisinden istifade edilmiş, sonuç olarak "Risk Tabanlı Çok Kriterli Karar Verme" yöntemi geliştirilmiştir. Numerik, esnek, objektif, kişiden bağımsız bu yöntem, İHA'lar konusunda Risk Analizi ve Çok Kriterli Karar Verme metodolojisini birlikte kullanmak açısından da yapılan ilk çalışmadır.

Literatür taramasında genel olarak karşılaşılan yöntemler, tam bir risk analizini veya değerlendirmesini içermeyip çoğunlukla risklerin bir olasılık olarak karar modeline dahil edilmesine ve alternatiflerin bu olasılıklar da göz önünde bulundurularak karşılaştırılmasına dayanırken bizim önerdiğimiz yöntemde farklı olarak, risk yönetiminin ilk adımı olan risk değerlendirmesi ve analizi tamamıyla icra edilmiş, bu amaçla ön tehlike listesi ve ön tehlike analizi metotları ile güvenlik blok diyagramı kullanılmış, sonucunda elde edilen tehlike listesi ve şiddet ile olasılığın çarpımı olarak ifade edilen risk çok kriterli karar verme yönteminde girdi olarak kullanılmıştır. Risk analizinden alınan tehlike listesi alternatifleri, risk ise alternatiflerin ağırlıklarını oluşturmuş, böylece risk analizi doğrudan kararı etkilemiştir.

Karar verme sürecinde, basitliği ve amaca uygunluğu nedeni ile Ağırlıklı Toplam Yöntemi çok kriterli karar verme modeli olarak belirlenmiş, hem tecrübe ve bilgiden hem de sayısal olgu ve verilerden istifade edilmek esas alındığından kalitatif ve kantitatif karışımı hibrit bir yaklaşım tercih edilmiştir. Karar matrisi oluşturulurken sayısal ağırlık ve oranlardan istifade edilmiş ancak bu ağırlık ve oranlar uzman grubun bilgi ve tecrübelerine dayalı olarak tespit edilmiştir. Karara niceliksel olarak ulaşabilmek adına alternatiflerin her bir kriteri ne oranda

karşıladığını belirlemek için “Kriter karşılama oranı-KKO” kullanılmıştır. Her bir kriter için ağırlık ve KKO çarpımı da “Değer” olarak isimlendirilmiştir.

Modelin uygulanması neticesinde; Açık Gönderme yönteminin zaten beklendiği üzere veri linki güvenliği açısından en zayıf yöntem olduğu, Yazılımsal Şifreleme ile Donanımsal Şifreleme alternatiflerinin aynı derecede ve tüm yöntemler göz önünde bulundurulduğunda ortalama seviyede güvenlik sağladığı, Kanal Şifreleme Yönteminin ilk üç alternatife kıyasla iyi seviyede veri linki güvenliği sağladığı, ancak önerilen metodunun diğer tüm yöntemlere kıyasla veri linki güvenliğinde yaklaşık % 6,6 iyileştirme sağladığı tespit edilmiştir.

Literatür taramasında karşılaşılan/tespit edilen diğer çalışmalarda videonun şifrelenmesi esas alınmış, veri linkinin güvenliği ikinci planda bırakılmıştır. Bu nedenle verilerin aktarıldığı linkin güvenliği ve sisteme giriş-çıkış prosedürü genellikle göz ardı edilmiştir. Yöntemimiz bu yaklaşımın tersine uçtan uca güvenliği esas almaktadır; ayrıca kablosuz veri aktarılan sadece hava aracı değil insansız kara ve deniz araçları için de kullanılabilmesi mümkündür.

Hangi yöntem kullanılırsa kullanılsın genel siber güvenlik açısından güvenlik duvarları ve antivirüs programları gibi yazılımların kullanılması ve mümkünse İHA sistemlerinin internet erişimi bulunmaması da önem arz etmektedir.

Bundan sonra yapılacak çalışmalarda yöntemin geliştirilmesi kapsamında; yeni bir şifreleme metodu geliştirilmesi, filigran uygulaması, kullanıcı ad ve şifrelerinin hash değerlerinin alınarak veri tabanında saklanması, şifre uzunluk ve karışıklık kontrolü yapılması, tek kullanımlık şifre (SMS, dongle, vb.) ilavesi ile iki aşamalı yetkilendirme teşkili, kullanıcı yetki, ad ve şifrelerinin belirli sürelerle yenilenmesi, bağlantı zaman ve sürelerinin tahdit edilmesi, tüm bağlantıların aynı zamanda kapatılmasına imkan veren panik butonu eklenmesi amaçlanmaktadır.

KAYNAKLAR

1. İnternet: İnsansız hava aracı. Web: http://tr.wikipedia.org/wiki/%C4%B0nsans%C4%B1z_hava_arac%C4%B1 30 Ocak 2017'de alınmıştır.

2. Qiao, L., Nahrsîedt, K. (1997, July). *A new algorithm for MPEG video encryption*. Paper presented at the First International Conference on Imaging Science, Systems and Technology, Nevada, LasVegas.

3. Wander, A.S., Gura, N., Eberle, H., Gupta, V. ve Shantz, S.C. (2005, March). *Energy analysis of public-key cryptography for wireless sensor networks*. Paper presented at the Third IEEE International Conference on Pervasive Computing and Communications, Kauai, Hawaii.

4. Xiao, Y., Rayi, V.K., Sun, B., Du, X., Hu, F. ve Galloway, M. (2007, 10 September). A survey of key management schemes in wireless sensor networks. *Computer Communications*, 30 (11-12), 2314-2341.

5. Ciprian, R., Nicolae, J., Constantin, B., Cosmin, A. (2008, May). Embedded real-time video encryption module on uav surveillance systems. *WSEAS Transactions on Circuits and Systems*, 7 (5), 368-381.

6. Chen, X., Makki, K., Yen, K. ve Pissinou, N. (2009). Sensor network security: a survey. *IEEE Communications Surveys & Tutorials*, 11 (2), 52-73.

7. Ren, K., Yu, S., Lou, W. ve Zhang, Y. (2009, October). Multi-user broadcast authentication in wireless sensor networks. *IEEE Transactions on Vehicular Technology*, 58 (8), 4554-4564.

8. Munivel, E., Ajit, G.M. (2010, 2-4 January). *Efficient public key infrastructure ımplementation in wireless sensor networks.* Paper presented at the International Conference on Wireless Communication and Sensor Computing, Chennai, India.

9. Robert, E., Guyot, V., Loica, A., Antoine. G., Laurent, B. (2012, 5-6 July). *Swarm UAV attack: how to protect sensitive data?.* Paper presented at the 11th European Conference on Information Warfare and Security, Laval, France.

10. Han, Y.H., Park, D.S., Jia, W., Yeo, S.S. (Editors). (2013). *Ubiquitous Information Technologies and Applications CUTE 2012 Volume 2014.* Berlin: Springer, 11-19.

11. Rodday, N. (2015, July). *Exploring security vulnerabilities of unmanned aerial vehicles*, Master Thesis, Faculty for Electrical Engineering, University of Twente, Amsterdam, 25-62.

12. İnternet: Wilson, A. (2015). Security: the key to affordable unmanned aircraft systems. *Wind River Systems*. INTEL Company. Web: https://www.windriver.com/whitepapers/aerospace-defense/security-the-key-to-affordable-unmanned-aircraft-systems/ adresinden 20 Nisan 2017'de alınmıştır.

13. Chen, X., Lifeng, W., Mengjiao, Z. ve Wemdong, W. (2016, January). A resource-efficient multimedia encryption scheme for embedded video sensing system based on unmanned aircraft. *Journal of Network and Computer Applications*, 59, 117-125.

14. Khadam, I.M., Kaluarachchi, J. (2003, September). Multi-criteria decision analysis with probabilistic risk assessment for the management of contaminated ground water. *Environmental Impact Assessment Review*, 23 (6), 683–721.

15. Khan, F.I., Sadıq, R., Haddara, M.H. (2004, November). Risk-based inspection and maintenance (RBIM) multi-attribute decision-making with aggregative risk analysis. *Process Safety and Environmental Protection*, 82 (6), 398–411.

16. Ying-Ming, W., Elhag, T.M.S. (2007, August). A fuzzy group decision making approach for bridge risk assessment. *Computers & Industrial Engineering*, 53 (1), 137–148.

17. Dillon, R.L., Liebe, R.M., Bestafka, T. (2009, March). Risk-based decision making for terrorism applications. *Society for Risk Analysis*, 29 (3), 321–335.

18. Ravindran, A.R., Bilsel, R.U., Wadhwa, V., Yang, T. (2010, 15 January). Risk adjusted multicriteria supplier selection models with applications. *International Journal of Production Research*, 48 (2), 405–424.

19. Catrinu, M.D., Nordgard, D.E. (2011, June). Integrating risk analysis and multi-criteria decision support under uncertainty in electricity distribution system asset management. *Reliability Engineering and System Safety*, 96 (6), 663–670.

20. Karmperis, A.C., Sotirchos, A., Aravossis, K., Tatsiopoulos, I.P. (2012, January). Waste management project's alternatives: a risk-based multi-criteria assessment (RBMCA) approach. *International Journal of Integrated Waste Management, Science and Technology*, 32 (1), 194–212.

21. Kuo, Y., Lu, S. (2013, May). Using fuzzy multiple criteria decision making approach to enhance risk assessment for metropolitan construction projects. *International Journal of Project Management*, 31 (4), 602–614.

22. İnternet: Unmanned aerial vehicle. Web: https://en.wikipedia.org/wiki/Unmanned_ aerial_vehicle 30 Ocak 2017'de alınmıştır.

23. İnternet: İHA pilotları böyle eğitiliyor. Web: http://www.aktuel.com.tr/dunya/2013/03 /02/iha-pilotlari-boyle-egitiliyor 30 Ocak 2017'de alınmıştır.

24. Kök, T. (2012). *İnsansız hava araçlarının güvenli kullanımı için spektrum ihtiyaçlarının belirlenmesi ile ilgili öneriler*. Teknik Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu, İstanbul, 9-11.

25. İnternet: SSM İHA sistemleri yol haritası (2011-2030). Web: http://www.ssm.gov.tr/_layouts/images/iha_ekatalog_web/index.html 20 Nisan 2017'de alınmıştır.

26. Akyürek, S., Yılmaz, M.A. Taşkıran, M. (2012, Aralık). *İnsansız hava araçları: muharebe alanında ve terörle mücadelede devrimsel dönüşüm.* Rapor No:53, BİLGESAM, Ankara.

27. İnternet: Yer kontrol istasyonu resmi. Web: http://www.israeli-weapons.com/ weapons/aircraft/uav/ hermes_ 180/Hermes_180.html 20 Nisan 2017'de alınmıştır.

28. İnternet: Yer kontrol istasyonu resmi, Web: http://priamtechcouk.ipage.com/ uploads/3/1/5/6/ 3156273/8883016_orig.jpg?695 20 Nisan 2017'de alınmıştır.

29. İnternet: Yer kontrol istasyonu resmi, Web: http://s130135561.onlinehome. us/files/img/uav/05-mq-9.jpg 20 Nisan 2017'de alınmıştır.

30. İnternet: Yer veri terminali resmi, Web: http://www.armyrecognition.com/europe /Hollande/Exhibition/Dutch_Army_Open_Days_2005/pictures/Grond_Data_Terminal _ArmyRecognition_Netherlands_01.jpg 20 Nisan 2017'de alınmıştır.

31. İnternet: yer veri terminali resmi, Web: http://www.revistaaerea.com/2009/08/04/ elisra-presents-new-data-link-technology-developments-for-uavs-at-this-years-auvsi/ 31 Ocak 2017'de alınmıştır.

32. Dursun, M., Aksöz, A. ve Saygın, A. (2015, 20-23 May). *A comparative study by PID and fuzzy control methods for flight parameters*. Paper presented at the Asian-Pacific Conference on Aerospace Technology and Science. Jeju Island, Korea.

33. İnternet: Uygunuçarlar, T. (2010). İnsansız hava araçlarında (İHA) veri iletim linkleri. *Savunma Sanayi Gündemi*, Sayı:12. Web: http://www.ssm.gov.tr/anasayfa/kurumsal/ SSM%20Dergisi/SSM_12_web.pdf adresinden 20 Nisan 2017'de alınmıştır.

34. Suraj, G.G., Mangesh, M.G., Jawandhiya, P.M. (2013, April). Review of unmanned aircraft system (UAS). *International Journal of Advanced Research in Computer Engineering & Technology*, 2 (4), 1646–1658.

35. İnternet: Raj, J., Fred, L.T. (2011). Wireless datalink for unmanned aircraft systems: requirements, challenges and design ideas. American Institute of Aeronautics and Astronautics. Web: http://www.cse.wustl.edu/~jain/papers/ftp/uas_dl.pdf adresinden 20 Nisan 2017'de alınmıştır.

36. İnternet: 5809 sayılı elektronik haberleşme kanunu. (Kasım, 2008). Web: http://www.udhb.gov.tr/udhbportal/udham.udhb.gov.tr/images/haricidosyalar/b6b1cd8 3fe79bdeK.pdf 20 Nisan 2017'de alınmıştır.

37. Ozkaya, B. (2011, February). *Application, comparison, and improvement of known received signal strength indication (RSSI) based indoor localization and tracking methods using active RFID device*, Master Thesis, METU Electrical and Electronics Engineering, Ankara, 38-53.

38. Adamy, D.L. (2008). *EW 103: Tactical battlefield communication electronic warfare*. London: Artech House, 27, 55-56, 169, 203-233.

39. Sklar, B. (2001). *Digital communications fundamentals and applications* (Second Edition). Los Angeles: Prentice Hall, 30-33.

40. Özeç, M.O. (2011, September). *Direction finding performance of antenna arrays on complex platforms using numerical electromagnetic simulation tools*, Master Thesis, METU Electrical and Electronics Engineering, Ankara, 1-6.

41. İpek, A.V. (2006, October). *Implementation of a direction finding algorithm on an FPGA platform*, Master Thesis, METU Electrical and Electronics Engineering, Ankara, 2-15.

42. Karadağ, S. (2014, September). *Experimental performance evaluation of direction finding by amplitude comparison for GSM applications*, Master Thesis, METU Electrical and Electronics Engineering, Ankara, 9-71.

43. Cheriet, A., Ouslim, M., Aizi, K. (2013). Localization in a wireless sensor network based on RSSI and a decision tree. *Przeglad Elektrotechniczny*, 89 (12), 121–125.

44. İleri, F. (2013). *RSSI based position estimation in zigbee sensor network*, Master Thesis, Boğaziçi University Electrical and Electronics Engineering, İstanbul, 1-4.

45. Yılmaz, A. (2015, February). *On localization and tracking using received signal strength measurements*, Master Thesis, METU Electrical and Electronics Engineering, Ankara, 15-33.

46. İnternet: Paganini, P. (June, 2013). Hacking drones overview of the main threats. *InfoSec Institute.* Web: http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/#gref adresinden 20 Nisan 2017'de alınmıştır.

47. İnternet: Daniel, S., Jahshan, A.B., Todd, E.H. (August, 2012). Drone hack: spoofing attack demonstration on a civilian unmanned aerial vehicle. *GPS World* Web: http://gpsworld.com/drone-hack/ adresinden 20 Nisan 2017'de alınmıştır.

48. Alan, K., Brandon, W., James, G., Inseok, H. (2012, 19-21 June). *Cyber attack vulnerabilities analysis for unmanned aerial vehicles*. Paper presented at the Infotech@Aerospace Conference, Garden Grove, California.

49. Kexiong, Z., Sreeraksha, K.R., Yaling, Y. (2014, 29-31 October). *Location spoofing attack and its countermeasures in database-driven cognitive radio networks*. Paper presented at the IEEE Conference on Communications and Network Security, San Francisco, CA.

50. Todd, E.H., Brent, M., Ledvina, Mark, L.P., Brady, W.O. Hanlon, P., Kintner, M,. (2008, 16-19 September). *Assessing the spoofing threat: development of a portable gps civilian spoofer*. Paper presented at the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation, Savannah, Georgia.

51. Andrew, J.K., Daniel, P.S., Jahshan, A.B., Todd, E.H. (2014, July). Unmanned aircraft capture and control via GPS spoofing. *Journal Journal of Field Robotics*, 31 (4), 617–636.

52. Tippenhauer, N.O., Popper, C., Rasmussen, K.B., Capkun, S. (2011, 17-21 October). *On the requirements for successful GPS spoofing attacks.* Paper presented at the 18th ACM Conference on Computer and Communications Security, Illinois, Chicago.

53. Georg T.B. (2009, 30 July). *Security mechanisms for positioning systems - enhancing the security of eLoran*, Master Thesis, Ruhr-Universitat Bochum, 13-15.

54. İnternet: Reading mission control data out of predator drone video feeds. Web: https://dl.packetstormsecurity.net/papers/general/Predator.pdf 20 Nisan 2017'de alınmıştır.

55. Todd, H. (2015, 18 March). *Statement on the security threat posed by unmanned aerial systems and possible countermeasures*. The University of Texas, Austin.

56. İnternet: Did Israel hack unmanned helicopter that entered their airspace?. Web: https://cyberarms.wordpress.com/2012/10/07/did-israel-hack-unmanned-helicopter-that-entered-its-airspace/ 28 Temmuz 2015'de alınmıştır.

57. İnternet: Lee, D. Drone aircraft hijacked by students in test; could Iran do it? Web: http://abcnews.go.com/Technology/hijacking-drone-uav-aircraft-texas-students-prove-hackers/story?id=16699686 03 Ağustos 2015'de alınmıştır.

58. İnternet: David, C. (November, 2013). German heron drone hacked and crashed by Taliban in Afghanistan. Web: http://theaviationist.com/2013/11/13/heron-hacked-afghanistan/ 28 Temmuz 2017'de alınmıştır.

59. İnternet: David, C. (December, 2011). Iran seizes a U.S. stealth drone by taking over controls. Maybe… and what about that Predator virus? Web: http://theaviationist.com/2011/12/04/iran-drone/ 19 Ağustos 2017'de alınmıştır.

60. İnternet: Hacked U.S. surveillance drone over Crimea shows new face of warfare. Web: http://www.homelandsecuritynewswire.com/dr20140411-hacked-u-s-surveillance-drone-over-crimea-shows-new-face-of-warfare 04 Ağustos 2015'de alınmıştır.

61. İnternet: Steven, F. (2014). Hacking and hijacking a drone. Web: https://urbantimes.co/2014/05/hacking-and-hijacking-a-drone/ 20 Ağustos 2015'de alınmıştır.

62. İnternet: Goodman, J.D. (December, 2015). Amid claims of more captured drones, a report on their vulnerability. Web: http://thelede.blogs.nytimes.com/2011/12/15/amid-claims-of-more-captured-drones-a-report-on-their-vulnerability/?_r=0 19 Ağustos 2015'de alınmıştır.

63. İnternet: UAV drones hacked by Iraqi insurgents. Web: http://anonhq.com/uav-drones-hacked-by-iraqi-insurgents/ 03 Ağustos 2017'de alınmıştır.

64. İnternet: Kevin, C. (February, 2015). How vulnerable are UAVs to cyber attacks?. Web: http://www.c4isrnet.com/story/military-tech/blog/net-defense/2015/02/23/drones-cyber-attack-threat/23883185/ 03 Ağustos 2017'de alınmıştır.

65. İnternet: Russoni M.A. Wondering how to hack a military drone? It's all on Google. Web: https:// http://www.ibtimes.co.uk/wondering-how-hack-military-drone-its-all-google-1500326 28 Temmuz 2017'de alınmıştır.

66. İnternet: Go programlama dili. Web: https://tr.wikipedia.org/wiki/Go_(programlama _dili) 22 Aralık 2016'da alınmıştır.

67. İnternet: Golang webcam library for Linux. Web: https://github.com/blackjack/webcam 2 Ocak 2017'de alınmıştır.

68. İnternet: Motion JPEG. Web: https://en.wikipedia.org/wiki/Motion_JPEG 25 Aralık 2016'da alınmıştır.

69. İnternet: RFC 5246: The transport layer security (TLS) protocol version 1.2. Web: https://tools.ietf.org/ html/rfc5246 20 Nisan 2017'de alınmıştır.

70. İnternet: RFC 1421: Privacy enhancement for internet electronic mail. Web: https://tools.ietf.org/html/rfc1421 20 Nisan 2017'de alınmıştır.

71. İnternet: RFC 4158: Internet X.509 public key ınfrastructure, Web: https://tools.ietf.org/html/rfc4158 20 Nisan 2017'de alınmıştır.

72. Fu, K., Sit, E., Smith, K., Feamster, N. (2001, 13-17 August). *Dos and don'ts of client authentication on the web*. Paper presented at the 10th USENIX Security Symposium, Washington, D.C.

73. Sarıkaya, K. (2011, 12-14 October). *Password-based client authentication for SSL/TLS protocol using elgamal and Chebyshev Polynomials*. Paper presented at the 5th International Conference on Application of Information and Communication Technologies, Baku, Azerbaijan.

74. Ericson, C.A. (2005). *Hazard analysis techniques for system safety*. New Jersey: John Wiley & Sons, 1-10, 55-57, 73-82.

75. İnternet: UAS safety risk assessment. (November, 2015). Web: https://www.droneii.com/uas-safety-risk-assessment 14 Şubat 2017'de alınmıştır.

76. Karakaşoğlu, N. (2008, Haziran). *Bulanık çok kriterli karar verme yöntemleri ve uygulama*, Yüksek Lisans Tezi, Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü, Denizli, 4-56.

77. Yılmaz, T., Kaygın, E., Gerekan, B. (2016, Kasım). Gıda maddeleri sanayii sektöründe faaliyet gösteren işletmelerin finansal performansının TOPSIS yöntemi ile ölçülmesi: BİST örneği. *Akademik Sosyal Araştırmalar Dergisi*, 33, 609–623.

78. Gülen, M. (2006, December). *İnsansız hava aracı kazalarının önlenmesinde örnek bir risk yönetimi uygulaması*, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 63-75.

79. Valavanis, K.P., Vachtsevanos, G.J. (Editors). (2014). *Handbook of unmanned aerial vehicles*. Berlin: Springer, 2229-2275.

80. Ağaç, G., Baki, B., Peker, İ., Ar, İ.M. (2015, Haziran). Çok kriterli karar verme tekniklerini kullanarak serbest bölge yer seçimi: Doğu Anadolu Bölgesi örneği. *Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 30 (1), 79–113.

EKLER

EK-1. Geliştirilen metoda ait GO kodu (main)

```
package main
import (
	"flag"
	"fmt"
	"log"
	"net/http"
	"os"
	"runtime"
	"sort"
	"sync"
	"github.com/blackjack/webcam")

var sessionStore *SessionStore
var mutex sync.RWMutex
var jpegImage []byte
var url = flag.String("url", "", "Camera host")
var addr = flag.String("addr", ":8080", "Server address")

func main() {
	flag.Parse()
	runtime.GOMAXPROCS(runtime.NumCPU())
	log.Println("Start streaming")
	cam, err := webcam.Open("/dev/video0")
	if err != nil {panic(err.Error())}
	defer cam.Close()
	format_desc := cam.GetSupportedFormats()
	var formats []webcam.PixelFormat
	for f := range format_desc { formats = append(formats, f)}
	println("Available formats: ")
	for i, value := range formats {fmt.Fprintf(os.Stderr, "[%d] %s\n", i+1,
format_desc[value])
	}
	choice := readChoice(fmt.Sprintf("Choose format [1-%d]: ", len(formats)))
	format := formats[choice-1]
	fmt.Fprintf(os.Stderr, "Supported frame sizes for format %s\n", format_desc[format])
	frames := FrameSizes(cam.GetSupportedFrameSizes(format))
	sort.Sort(frames)
	for i, value := range frames {
		fmt.Fprintf(os.Stderr, "[%d] %s\n", i+1, value.GetString())
	}
	f, w, h, err := cam.SetImageFormat(format, 640, 480)
	if err != nil {panic(err.Error())} else {
		fmt.Fprintf(os.Stderr, "Resulting image format: %s (%dx%d)\n", format_desc[f],
		w, h)}
	fmt.Println("Starting streaming")
	err = cam.StartStreaming()
	if err != nil {panic(err.Error())}
	timeout := uint32(5) //5 seconds
```

EK-1.(devam) Geliştirilen metoda ait GO kodu (main)

```
go func() {
	for {
		err = cam.WaitForFrame(timeout)
		switch err.(type) {
		case nil:
		case *webcam.Timeout:
			fmt.Fprint(os.Stderr, err.Error())
			continue
		default:
			panic(err.Error())}
		frame, err := cam.ReadFrame()
		if len(frame) != 0 {
			mutex.Lock()
			jpegImage = frame
			mutex.Unlock()
		} else if err != nil {
			panic(err.Error())} }
	}()

	http.HandleFunc("/", IndexHandler)
	http.HandleFunc("/login", LoginHandler)
	http.HandleFunc("/logout", LogoutHandler)
	http.HandleFunc("/snapshot", SnapshotHandler)
	http.HandleFunc("/live", VideoHandler)
	http.HandleFunc("/jpeg", JpegHandler)
	http.HandleFunc("/mjpeg", MotionJpegHandler)
	http.ListenAndServe(*addr, nil)}

func readChoice(s string) int {
	var i int
	for true {
		print(s)
		_, err := fmt.Scanf("%d\n", &i)
		if err != nil || i < 1 {
			println("Invalid input. Try again")
		} else {break}
	}
	return i
}

type FrameSizes []webcam.FrameSize
func (slice FrameSizes) Len() int {return len(slice)}
func (slice FrameSizes) Less(i, j int) bool {
	ls := slice[i].MaxWidth * slice[i].MaxHeight
	rs := slice[j].MaxWidth * slice[j].MaxHeight
	return ls < rs
}
```

EK-1.(devam) Geliştirilen metoda ait GO kodu (main)

```
func (slice FrameSizes) Swap(i, j int) {
	slice[i], slice[j] = slice[j], slice[i]}
func init() {
	sessionStore = NewSessionStore()}
```

EK-2. Geliştirilen metoda ait GO kodu (handlers)

```
package main
import (
	"bytes"
	"fmt"
	"log"
	"mime/multipart"
	"net/http"
	"net/textproto")

func IndexHandler(w http.ResponseWriter, r *http.Request) {
	data := make(map[string]interface{})
	cookie, err := r.Cookie("sid")
	if err == nil {
		session := sessionStore.Get(cookie.Value)
		if session.isNew == false {
			data["user"] = session.value["user"]}
	}
	renderTemplate(w, "index.html", data)
}

func VideoHandler(w http.ResponseWriter, r *http.Request) {
	cookie, err := r.Cookie("sid")
	if err != nil {
		http.Redirect(w, r, "/login", 302)
		return}
	session := sessionStore.Get(cookie.Value)
	if session.isNew {
		http.Redirect(w, r, "/login", 302)
		return}
	session.Update()
	data := make(map[string]interface{})
	data["user"] = session.value["user"]
	renderTemplate(w, "video.html", data)
}

func SnapshotHandler(w http.ResponseWriter, r *http.Request) {
	cookie, err := r.Cookie("sid")
	if err != nil {
		http.Redirect(w, r, "/login", 302)
		return}
	session := sessionStore.Get(cookie.Value)
	if session.isNew {
		http.Redirect(w, r, "/login", 302)
		return}
	session.Update()
	data := make(map[string]interface{})
	data["user"] = session.value["user"]
	renderTemplate(w, "snapshot.html", data)}
```

EK-2.(devam) Geliştirilen metoda ait GO kodu (handlers)

```
func LoginHandler(w http.ResponseWriter, r *http.Request) {
	data := make(map[string]interface{})
	if r.Method == "GET" {
		renderTemplate(w, "login.html", data)}
	if r.Method == "POST" {
		username := r.FormValue("username")
		password := r.FormValue("password")
		loggedin := false
		if user, ok := FindUser(username, password); ok {
			fmt.Println(user)
			session := NewSession(map[interface{}]interface{}{"user": user})
			session.isNew = false
			sessionStore.Set(session.sid, session)
			cookie := &http.Cookie{Name: "sid", Value: session.sid}
			http.SetCookie(w, cookie)
			loggedin = true
			http.Redirect(w, r, "/", 302)}
		data["username"] = username
		data["errorMessage"] = "Kullanıcı Adı veya Şifresi Hatalı"
		if !loggedin {
			renderTemplate(w, "login.html", data)}
	}
}

func LogoutHandler(w http.ResponseWriter, r *http.Request) {
	cookie, err := r.Cookie("sid")
	if err == nil {
		sessionStore.Delete(cookie.Value)
		cookie := &http.Cookie{Name: "sid", Value: "", MaxAge: -1}
		http.SetCookie(w, cookie)
		http.Redirect(w, r, "/", 302)
		return}
	http.Redirect(w, r, "/", 302)
}

func JpegHandler(w http.ResponseWriter, r *http.Request) {
	cookie, err := r.Cookie("sid")
	if err != nil {
		http.Redirect(w, r, "/login", 302)
		return	}
	session := sessionStore.Get(cookie.Value)
	if session.isNew {
		http.Redirect(w, r, "/login", 302)
		return	}

	session.Update()
	w.Header().Set("Content-Type", "image/jpeg")
	w.Header().Set("cache-control", "priviate, max-age=0, no-cache")
```

EK-2.(devam) Geliştirilen metoda ait GO kodu (handlers)

```
	w.Header().Set("pragma", "no-cache")
	w.Header().Set("expires", "-1")
	w.Write(jpegImage)
}

func MotionJpegHandler(w http.ResponseWriter, r *http.Request) {
	cookie, err := r.Cookie("sid")
	if err != nil {
		http.Redirect(w, r, "/login", 302)
		return}

	session := sessionStore.Get(cookie.Value)
	if session.isNew {
		http.Redirect(w, r, "/login", 302)
		return}
	session.Update()
	log.Println("Serve streaming")
	m := multipart.NewWriter(w)
	w.Header().Set("Content-Type", "multipart/x-mixed-replace;
boundary="+m.Boundary())
	w.Header().Set("Connection", "close")
	w.Header().Set("cache-control", "priviate, max-age=0, no-cache")
	w.Header().Set("pragma", "no-cache")
	w.Header().Set("expires", "-1")
	header := textproto.MIMEHeader{}
	var buf bytes.Buffer
	for {
		mutex.RLock()
		buf.Reset()
		_, err := buf.Write(jpegImage)
		mutex.RUnlock()
		if err != nil {
			break}
		header.Set("Content-Type", "image/jpeg")
		header.Set("Content-Length", fmt.Sprint(buf.Len()))
		mw, err := m.CreatePart(header)
		if err != nil {
			break}
		mw.Write(buf.Bytes())
		if flusher, ok := mw.(http.Flusher); ok {
			flusher.Flush()}
	}
	log.Println("Stop streaming")
}
```

EK-3. Geliştirilen metoda ait GO kodu (init)

```
package main
import (
	"errors"
	"html/template"
	"net/http")

var templates map[string]*template.Template
var ErrTemplateDoesNotExist = errors.New("The template does not exist.")
func renderTemplate(w http.ResponseWriter, name string, data map[string]interface{})
error {
	tmpl, ok := templates[name]
	if !ok {
		return ErrTemplateDoesNotExist
	}
	tmpl.ExecuteTemplate(w, "base", data)
	return nil}

func init() {
	if templates == nil {
		templates = make(map[string]*template.Template)
	}
	templates["index.html"] = template.Must(template.ParseFiles("templates/base.html",
"templates/index.html", "templates/navigation.html"))
	templates["login.html"] = template.Must(template.ParseFiles("templates/base.html",
"templates/login.html", "templates/navigation.html"))
	templates["information.html"] =
template.Must(template.ParseFiles("templates/base.html", "templates/information.html",
"templates/navigation.html"))
	templates["snapshot.html"] =
template.Must(template.ParseFiles("templates/base.html", "templates/snapshot.html",
"templates/navigation.html"))
	templates["video.html"] = template.Must(template.ParseFiles("templates/base.html",
"templates/video.html", "templates/navigation.html"))
}
```

EK-4. Geliştirilen metoda ait GO kodu (session)

```
package main
import (
	"crypto/rand"
	"encoding/base64"
	"io"
	"sync"
	"time")

type SessionStore struct {
	sync.Mutex
	sessions map[string]*Session}
func NewSessionStore() *SessionStore {
	return &SessionStore{sessions: make(map[string]*Session)}}
func (ss *SessionStore) Set(sid string, session *Session) {
	ss.Lock()
	defer ss.Unlock()
	ss.sessions[sid] = session}
func (ss *SessionStore) Get(sid string) *Session {
	ss.Lock()
	defer ss.Unlock()
	if v, ok := ss.sessions[sid]; ok {
		v.timeAccessed = time.Now()
		return v   }
	return &Session{isNew: true}}
func (ss *SessionStore) Delete(sid string) {
	delete(ss.sessions, sid)}
func (ss *SessionStore) Reset() {
	ss.Lock()
	defer ss.Unlock()
	ss.sessions = make(map[string]*Session)}
func (ss *SessionStore) GC() {
	ss.Lock()
	defer ss.Unlock()
	for sid, session := range ss.sessions {
		if (session.timeAccessed.Unix() + session.maxLifetime) < time.Now().Unix() {
			delete(ss.sessions, sid)}
	}
}
type Session struct {
	sync.Mutex
	sid          string                     // unique session id
	timeCreated  time.Time                  // last access time
	timeAccessed time.Time                  // last access time
	value        map[interface{}]interface{} // session value stored inside
	isNew        bool
	maxLifetime  int64}

func (s *Session) Update() {
```

EK-4.(devam) Geliştirilen metoda ait GO kodu (session)

```
	s.Lock()
	defer s.Unlock()
	s.timeAccessed = time.Now()}

func NewSession(value map[interface{}]interface{}) *Session {
	s := &Session{}
	s.sid = CreateSessionId()
	s.timeCreated = time.Now()
	s.value = value
	s.isNew = true
	return s}

func CreateSessionId() string {
	b := make([]byte, 32)
	if _, err := io.ReadFull(rand.Reader, b); err != nil {
		return ""}
	return base64.URLEncoding.EncodeToString(b)}
```

EK-5. Geliştirilen metoda ait GO kodu (user)

```
package main
import "strings"

var Users = []User{
	User{"icuhadar", "İsmet ÇUHADAR", "icuhadar1", false, true, false},
	User{"mdursun", "Mahir DURSUN", "mdursun1", false, true, false},
	User{"user", "Tanımlanmamış", "password", false, false, false},
}

type User struct {
	Username   string
	FullName   string
	Password   string
	IsDisabled bool
	IsAdmin    bool
	IsLoggedin bool
}

func FindUser(username, password string) (User, bool) {
	for _, user := range Users {
		if strings.Compare(user.Username, username) == 0 &&
strings.Compare(user.Password, password) == 0 {
			return user, true}
	}
	return User{}, false
}
```

EK-6. Geliştirilen metoda ait GO kodu (template/base)

```
{{define "base"}}
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="icon" href="./static/favicon.ico">
<style>

ul {
      list-style-type: none;
      margin: 0;
      padding: 0;
      overflow: hidden;
      background-color: #333;
     }
li {float: left;}
li a {
      display: block;
      color: white;
      text-align: center;
      padding: 14px 16px;
      text-decoration: none;
     }
li span {
      display: block;
      color: yellow;
      text-align: center;
      padding: 14px 16px;
      text-decoration: none;
     }
li a:hover:not(.active) {background-color: #111;}

.active {background-color: #4CAF50; }
</style>
<title>{{.title}}</title>
</head>
<body>
      {{template "navigation" .}}
      {{template "body" .}}
</body>
</html>
{{end}}
```

EK-7. Geliştirilen metoda ait GO kodu (template/index)

```
{{define "body"}}
<h3>Buraya giriş sayfasında bulunamı istenilen şeyler yazılacak.</h3>
{{end}}
```

EK-8. Geliştirilen metoda ait GO kodu (template/information)

```
{{define "body"}}
<h1>Sistem Bilgileri</h1>
{{end}}
```

EK-9. Geliştirilen metoda ait GO kodu (template/login)

```
{{define "body"}}
<h3>Kullanıcı Girişi</h3>
<form method="post" action="./login">
<div class="form-group">
<label for="username">Kullanıcı Adı</label><br>
<input type="text" name="username" class="form-control" id="username">
</div>
<div class="form-group">
<label for="password">Şifre</label><br>
<input type="password" name="password" class="form-control" id="password">
</div>
<button type="submit" class="btn btn-primary">Giriş</button>
<div style="color:red; font-size: larger;">{{.errorMessage}}</div>
</form>
</form>
{{end}}
```

EK-10. Geliştirilen metoda ait GO kodu (template/navigation)

```
{{define "navigation"}}
<ul>
<li><a class="active" href="/">Ana Sayfa</a></li>
<li><a href="/snapshot">Anlık Görüntü</a></li>
<li><a href="/live">Canlı Görüntü</a></li>
<li><a href="/info">Sistem Bilgileri</a></li>

{{if .user}}
<li><span>Kullanıcı: {{.user.FullName}}</span></li>
<li><a href="/logout">Çıkış</a></li>
{{else}}
	<li><a href="/login">Üye Girişi</a></li>
{{end}}
</ul>
{{end}}
```

EK-11. Geliştirilen metoda ait GO kodu (template/snapshot)

```
{{define "body"}}
<img src="/jpeg"/>
{{end}}
```

EK-12. Geliştirilen metoda ait GO kodu (template/video)

```
{{define "body"}}
<img src="/mjpeg"/>
{{end}}
```

EK-13. Şifresiz kanal ile etkinleştirilmiş görüntü aktarım GO kodu

```
package main
import (
	"fmt"
	"log"
	"mime/multipart"
	"net/http"
	"net/textproto"
	"os"
	"sync"
	"github.com/blackjack/webcam")

func main() {
	var mutex sync.RWMutex
	var jpegImage []byte
	framesay:=0
	gondermesay:=0
	cam, err := webcam.Open("/dev/video0")
	if err != nil {panic(err.Error())}
	defer cam.Close()
	cam.SetImageFormat(1196444237, 960, 540)
	if err != nil {panic(err.Error())}
	fmt.Println("Video Formatı: Motion JPEG (960 x 540)\n")
	log.Println("Video Akışı  Hazır\n")
	err = cam.StartStreaming()
	if err != nil {panic(err.Error())}
	timeout := uint32(5)

go func() {

	for {
		err = cam.WaitForFrame(timeout)
		switch err.(type) {
		case nil:
		case *webcam.Timeout:
		fmt.Fprint(os.Stderr, err.Error())
		continue
		default:
		panic(err.Error())
		}
	frame, err := cam.ReadFrame()
		if len(frame) != 0 {
			mutex.Lock()
			jpegImage = frame
			mutex.Unlock()
			log.Println("framesay:  ", framesay)
			framesay++
		} else if err != nil {panic(err.Error())}	}
	}()
```

EK-13.(devam) Şifresi kanal ile etkinleştirilmiş görüntü aktarım GO kodu

```
http.HandleFunc("/jpeg", func(w http.ResponseWriter, r *http.Request) {
w.Header().Set("Content-Type", "image/jpeg")
w.Write(jpegImage)})

http.HandleFunc("/mjpeg", func(w http.ResponseWriter, r *http.Request) {
log.Println("Video Akışı Başladı")
m := multipart.NewWriter(w)
w.Header().Set("Content-Type", "multipart/x-mixed-replace;
boundary="+m.Boundary())
w.Header().Set("Connection", "close")
header := textproto.MIMEHeader{}

for {
    if gondermesay<framesay{
        gondermesay=framesay
        log.Println("gondermesay:  ", gondermesay)
        header.Set("Content-Type", "image/jpeg")
        header.Set("Content-Length", fmt.Sprint(len(jpegImage)))
        mw, err := m.CreatePart(header)
        if err != nil {break}
        _, err = mw.Write(jpegImage)
        if err != nil {break}
        if flusher, ok := mw.(http.Flusher); ok {
            flusher.Flush()}
        }
    }
    log.Println("Video Akışı Bitti\n")
})

http.HandleFunc("/", func(w http.ResponseWriter, r *http.Request) {
w.Header().Set("Content-Type", "text/html")
w.Write([]byte(`<img src="/mjpeg" />`))
})

http.ListenAndServe(":8080", nil)}
```

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: Çuhadar, İsmet
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 08.03.1978, Konya
Medeni hali	: Evli
Telefon	: 0 (544) 303 07 13
Faks	: -
e-mail	: ismetcuhadar@gmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Doktora	Gazi Üniversitesi /Kazaların Çevresel ve Teknik Araştırması ABD	2017
Yüksek lisans	ODTÜ /Enformatik Enstitüsü Modelleme ve Simülasyon Bölümü	2006
Lisans	Kara Harp Okulu /Sistem Mühendisliği	2000
Lise	Maltepe Askeri Lisesi	1996

İş Deneyimi

Yıl	Yer	Görev
2000-2017	Kara Kuvvetleri Komutanlığı	Subay

Yabancı Dil

İngilizce

Yayınlar

1. Çuhadar, İ., Dursun, M. (2015, 20-23 May). *The aspects, reasons and outcomes of an unmanned air vehicle crash caused by engine failure*. Paper presented at the 8th Asian-Pacific Conference on Aerospace Technology and Science, Jeju Island, Korea.

2. Çuhadar, İ., Dursun, M. (2015). The aspects, reasons and outcomes of an unmanned air vehicle crash caused by engine failure. *International Journal of Aerospace System Engineering,* 2 (1), 1-5.

3. Çuhadar, İ., Dursun, M., Aksöz, A. (2015, 11-12 Kasım). *İnsansız bir hava aracı modelinin üç boyutlu tasarımı, analizi ve simülasyonu*. 6. Ulusal Savunma Uygulamaları Modelleme ve Simülasyon Konferansında sunuldu, Ankara.

4. Çuhadar, İ., Dursun, M. (2016, 20-23 May). *Unmanned air vehicle system's data links*. Paper presented at the 2nd International Conference on Electrical and Electronics Engineering, Ankara.

5. Çuhadar, İ., Dursun, M. (2016, June). Unmanned air vehicle system's data links. *Journal of Automation and Control Engineering,* 4 (3), 189-193.

Hobiler

Spor yapmak, kitap okumak, teknolojik gelişmeleri takip etmek.

DİZİN

GAZİ GELECEKTİR...