İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

GÜVENLİ ŞEKİLDE DOST UÇAKLARI TANIMA

YÜKSEK LİSANS TEZİ

Buse TEKİN AYDIN

Bilişim Uygulamaları Anabilim Dalı

Bilgi ve Haberleşme Mühendisliği Programı

Tez Danışmanı: Doç. Dr. Enver Özdemir

HAZİRAN 2019

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

GÜVENLİ ŞEKİLDE DOST UÇAKLARI TANIMA

YÜKSEK LİSANS TEZİ

Buse TEKİN AYDIN
(708151005)

Bilişim Uygulamaları Anabilim Dalı

Bilgi ve Haberleşme Mühendisliği Programı

Tez Danışmanı: Doç. Dr. Enver Özdemir

HAZİRAN 2019

İTÜ, Bilişim Enstitüsü'nün 708151005 numaralı Yüksek Lisans Öğrencisi Buse TEKİN AYDIN, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "GÜVENLİ ŞEKİLDE DOST UÇAKLARI TANIMA" başlıklı tezini aşağıdaki imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Doç. Dr. Enver Özdemir** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Doç. Dr. Ergün YARANERİ** İstanbul Teknik Üniversitesi	.....
	Dr. Öğr. Üyesi Elif Segah ÖZTAŞ Karamanoğlu Mehmetbey Üniversitesi	.....
		.....

Teslim Tarihi : **29 Nisan 2019**
Savunma Tarihi : **14 Haziran 2019**

Eşime ve aileme,

ÖNSÖZ

Tez konusunu seçerken isteklerimi göz önünde bulundurup bana yardımcı olan tez danışmanım Doç. Dr. Enver Özdemir'e teşekkürlerimi sunarım. Tez yazma sürecinde bana destek olan beni motive eden eşime, tüm eğitim hayatım boyunca benden maddi ve manevi desteklerini esirgemeyen, her zaman yanımda olan sevgili babama, anneme, kardeşime ve bu süreçte yanımda olan tüm dostlarıma teşekkürlerimi bir borç bilirim.

Haziran 2019 Buse TEKİN AYDIN

İÇİNDEKİLER

Sayfa

KISALTMALAR

ADS-B : Otomatik Bağımlı Gözetim Yayını
ATC : Hava Trafik Kontrolü
ATM : Hava Trafik Yönetimi
CAA : Sivil Havacılık Otoritesi
CNI : Haberleşme Navigasyon Tanıma
DoD : Amerika Birleşik Devletleri Savunma Bakanlığı
EUROCAE : Sivil Havacılık Donanımı Avrupa Kurumu
FAA : Federal Havacılık İdaresi
FRUIT : Eşzamanlı Olmayan Yanıtlar
GNSS : Global Navigasyon Uydu Sistemi
ICAO : Uluslararası Havacılık Örgütü
ICT : Bilgi ve İletişim Teknolojileri
IFF : Dost Düşman Tanıma Sistemi
IFR : Aletli Uçuş Kuralları
NextGen : Yeni Nesil Havacılık Sistemi
PKI : Açık Anahtarlı Kriptografik Yöntemler
PPI : Plan Durum Göstergesi
PPM : Darbe Konum Modülasyonu
PSR : Birincil Gözetim Radarı
RTCA : Radyo Havacılık Teknik Komisyonu
SDR : Yazılım Tabanlı Radyo
SESAR :Tek Avrupa Seması ATM Araştırma Programı
SIF : Seçici Kimlik Tanıma Özelliği
SSR : İkincil Gözetim Radarı
TCAS : Trafik Çarpışma Kaçınma Sistemi
VFR : Görerek Uçuş Kuralları
ZKP : Sıfır Bilgi İspatı

SEMBOLLER

μs	**:** Mikrosaniye
MHz	**:** MegaHertz

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

GÜVENLİ ŞEKİLDE DOST UÇAKLARI TANIMA

ÖZET

Son yıllarda havacılık sektörünün popülerliği hem sivil hem de askeri alanda artmıştır. Sivil havacılıkta kullanımları yoğun bir şekilde devam eden ve her geçen yıl kullanımları giderek artan yolcu taşıma uçaklarına, kargo taşıma uçaklarına ek olarak; insansız hava araçları gibi araçların giderek yaygınlaşmaya başlaması ve drone gibi yeni nesil insansız hava araçlarının da popülerliğinin artması (gözlem ve insan-yük taşıma faaliyetlerindeki kullanımlarının artması) bu sektörü her geçen yıl daha da güçlü kılmaktadır ve sektörün zorlukları da giderek artmaktadır. Askeri havacılıkta ise kullanımları yıllardır süregelen savaş uçakları, helikopterler gibi hava araçlarına ek olarak; yine gözlem için kullanılan insansız hava araçları ve savunma-saldırı için kullanılan silahlı insansız hava araçları, askeri havacılık alanını devletler için takip edilmesi kaçınılmaz bir alan kılmaktadır. Sektörün mevcut alanlarındaki hava araçlarının kullanımının artması ve yeni hava araçlarının kullanılmaya başlanması her ne kadar herkesi memnun etse de, artan trafiğin yönetiminin her geçen gün zorlaşması sektörün sorunlarından bir tanesi haline gelmiştir. Ayrıca artan bu kullanımla birlikte güvenlik konusu da gittikçe önem kazanmaktadır. Bu çalışmamızda savaş uçaklarında bulunan dost - düşman tanıma sistemlerine alternatif olabilecek aynı zamanda sivil havacılıktaki güvenlik problemlerini de giderebilecek bir tanıma şeması geliştirdik.

Bu tezde yetkisi olmayan uçakların kendilerini diğer uçaklara "dost" olarak tanıtmasını engellemek amacıyla uçak filoları arasında kullanılabilecek bir tanıma (identification) şeması tasarlanmıştır. Bu şema havacılık iletişimdeki tanıma sorununa bir çözüm olarak kullanılabilir. Yöntemimiz klasik şifreleme yöntemlerinin ve sıfır bilgi ispatı yöntemlerinin bir birleşimidir. Dost filolarda yer alan uçaklara, aynı filo içinde yer alan uçaklara aynı anahtarlar dağıtılmak üzere, birbirleriyle belirlenen benzerlik oranında benzeşen gömülü anahtarlar dağıtılmış ve kullandığımız matematiksel modelle iki filo arasında anahtarlarının benzerliğini anlama kıstası üzerinden bir tanımlama şeması tasarlanmıştır. Zero Knowledge Proof tekniği sayesinde iki hava aracı arasında gömülü anahtarına dair hiçbir bilgi paylaşımı olmadan "dost" veya "bilinmeyen" olarak kategorileştirme işlemi yapılması amaçlanmıştır. Dost kategorisine giren hava araçlarının mesajları bu iletişim sonrasında işlenirken, bilinmeyen olarak işaretlenen hava araçlarının mesajlarının dikkate alınmaması sağlanacaktır. Genel olarak bu çalışmada sıfır bilgi ispatına dayanan yöntemle daha güvenilir bir tanıma sistemi sistem sunduk.

SECURE IDENTIFICATION FRIENDLY AIRCRAFT

SUMMARY

In last years, aviation industry has become more and more popular. In addition to being extensively used in air transportation and cargo transportation areas which are continuing to be used intensively in civil aviation; the increasing popularity of new generation unmanned aerial vehicles such as drone (observation, human-cargo transport activities) makes this sector stronger and more challenging every year. Besides, the air vehicles such as combat aircraft, helicopters, which have been in use for years in military aviation; the unmanned aerial vehicles that used for observation and armed unmanned aerial vehicles that used for defense-attack make the military aviation an inevitable subject to follow closey.

Technological developments have undoubtedly improved their accuracy, consistency, effectiveness and system continuity of aviation navigation systems. System security has become a necessity in the sector to eliminate the threats of the aviation infrastructure. Currently, there is no common vision, common strategy, objectives, standards, implementation models or international policies defining cyber security for commercial aviation. It is a common responsibility of governments, airlines, airports and manufacturers to ensure a safe aviation system and prevent cyber threats.

Avionics which means aviation electronics covers all electronic systems used in an aircraft. These systems mainly perform navigation, communication, display and other flight and duty functions. Military avionics systems are indispensable for manned, unmanned aircraft, missiles and weapons. These systems allow the aircraft to perform defense, attack and surveillance tasks. The main difference between the Avionics software and the conventional embedded software is that the avionic software is optimized for security and the legal arrangements that require the development process of the software. Avionics become an important discipline with the rapid development of new generation computers, communication hardware, software languages and development tools. With these developing areas, the avionics has expanded and become multi-disciplined.

Although increased usage of vehicles in the existing areas and the newly coming aircrafts pleased everyone, overseeing and controlling of air traffic has become one of the biggest problems in the sector. Even if we have developed PSR (Primary Surveillance Radar) and SSR (Secondary Surveillance Radar) to control the air traffic, afterwhile these developed technologies become insufficient because of the increased aircrafts. These radar systems were highly costly and inappropriate for the newly coming air vehicles. In these radar systems, the vehicles has to communicate with the ATC (Air Traffic Controller) tower to inform other air crafts and also has to communicate with ATC tower again to get the information from other air crafts. In order for the ATC towers to manage the airspace safely, each control unit must

understand the status of each aircraft. Traditionally, the PSR and the SSR have fulfilled this role in various ways since World War II. Both systems are designed at a time when radio transmission requires a great deal of financial investment and expertise. Therefore, these old systems were not given any security considerations because they were assumed to be inaccessible. The rise of Software-Based Radio (SDR) overrides this assumption and has enabled potential attackers to compromise the system with fewer resources. Without authentication of the basic protocols, data link level attacks are more difficult to detect for both aviation systems and users of these systems than for attacks on traditional analog technologies such as the audio communication system or primary surveillance radar (PSR).

A new communication technology named ADS-B (Automatic Dependent Surveillance-Broadcast) has developed and started to be used in air craft vehicles. Using the global navigation system, ADS-B helps aircraft find their position independently. Aircrafts can periodically send their altitude, speed and other relevant data with the help of a digital data connection that communicates with air-to-air and air-to-land systems. ADS-B is a completely new paradigm for air traffic control. Each participant gets their position and speed using a built-in GPS (Global Positioning System) receiver. The location is then periodically broadcasted by a transmitter subsystem called ADS-B Out with a message (typically twice per second). The messages are received and processed by ATC towers on the ground or by nearby aircraft if the air craft is equipped with ADS-B In. One of the security problem of ADS-B is that it is impossible to detect the identification of the ADS-B message sender aircraft.

The critical importance of IFF (Identification Friend or Foe) systems has led to many studies for it. IFF system is installed in vehicles such as warplanes and warships. It is a radar transponder that responds correctly with an encrypted message that describes the aircraft or ship “friend” when interrogated by appropriate radar signal. Interrogative devices are placed in search, surveillance and capture radars. It is also installed in the guidance systems of certain antiaircraft missiles. All aircraft and ships equipped with the IFF may be targetted if they do not react correctly when detected by the radar. In Air Defense Systems, identification and access control of friendly-foe aircraft are the necessary protection mechanisms.

Furthermore, security in communication is becoming more and more important with this increased usage. We have created an identification scheme that can be an alternative to the identification of friend or foe systems in combat aircraft, which can also solve the security problems in civil aviation.

There are many different algorithms that provide secure communication in cryptography. In this study, we will use two algorithms, namely Secret Sharing and Zero Knowledge Proof (ZKP). ZKP systems were introduced in 1985 by Goldwasser, Micali and Rackoff. This protocol is based on a Prover convincing a Verifier to validate knowledge without revealing any information beyond the reality of information. ZKP techniques are important techniques used in cryptographic algorithms.

Interpolation is a basic mathematical technique to bring something complicated to a simple or at least less complex structure.Interpolation is an effective tool to make high precision approximations. These methods generally provide numerical approaches to calculate complex function values and to evaluate differential equations. Polynomial interpolation methods date back to 17th century. Polynomial interpolation provides a

simple and good way to predict the analytical expression, specifically a function, in a region stretched by the measured points. The Newton Divided Difference method is a numerical procedure that is used to interpolate a given set of points.

In this thesis, an identification scheme that can be used between aircraft fleets is designed to prevent unauthorized aircraft from introducing themselves as "friends" to other aircraft. This scheme can be used as a solution to the identification problem in aviation communication. Our method is a combination of classical encryption methods and zero knowledge proof methods. The method we recommend is not as complicated as other ZKP methods using graph isomorphism. Moreover, it is not only available for military aircraft. The identification scheme which we use can also be used by other non-aeronautical systems, eg on IoT devices. Because we do not use time-varying IFF codes, the cost of implementation is lower than other methods. This also makes the operational cost lower. It is more reliable for secret listening attacks. Because we use the ZKP, the attacker cannot capture or manipulate any confidential information.

In this method, embedded keys similar to each other with the already agreed similarity ratio are distributed to the aircraft in the friendly fleets. The same keys were distributed to the aircrafts in the same fleet. Thanks to the mathematical model designed the identification scheme provides a method to understand the similarity ratio of the keys between the two aircrafts. In this method, both sides (interrogating and responding) make polynomial interpolation with the values installed or given. Interrogator investigates whether the value calculated with a set of values at a certain point is the same as the responder part. When the values taken from responder includes the one that was calculated after interpolating polynomial, the responder is marked as “friend”. If the set of values doesn’t include the value calculated by interrogator, then the responder is marked as “foe”. The Zero Knowledge Proof technique made it possible to mark an aircarft vehicle “friend” or “foe” without sharing any information about their embedded keys.

Thanks to this method, the messages of the aircrafts that belong to “friend” category will be processed after this communication and the messages of the aircraft marked as “unknown” will be ignored.

In general, we have presented a more reliable identification system in this study which is based on zero knowledge proof and classical encryption methods.

The software to be used in this identification model that we have developed can be dealt with in future studies in a way that is in compliance with DO-178B standard.

1. GİRİŞ

Havacılık, 1903 yılında Wright kardeşlerin tarihteki ilk uçuşunu yaptığı andan itibaren sürekli gelişmektedir. Birinci Dünya Savaşı sırasında savaş için daha iyi uçaklara sahip olma çabasıyla gelişme daha da artmıştır. Sadece uçak teknolojisini geliştirme ihtiyacı değil, aynı zamanda hava alanını kontrol etmenin de gereksinimi doğmuştur. [5]

Havacılık endüstrisi giderek genişliyor, değişiyor ve daha fazla bağlantı kuruyor. Dünyanın en karmaşık ve bütünleşmiş bilgi ve iletişim teknolojileri sistemlerinden biri olan küresel havacılık sistemi, büyük ölçekli bir siber saldırı için potansiyel bir hedeftir. Havacılık endüstrisi, yeni teknolojilerin sürekli ve hızlı entegrasyonuyla genişlemeye, değişmeye ve giderek daha fazla bağlantı kurmaya devam ediyor. Böylece operasyonlar daha hızlı ve daha güvenilir hale geliyor. Ancak, teknoloji hızla geliştikçe, rakiplerimiz ve tehditleri de değişiyor ve gelişiyor. Havacılık endüstrisi, bu gelişen tehditleri ele almak için uygun siber güvenlik önlemleri almadığında risk altında olabilir. Bu nedenle, havacılık endüstrisinin en yüksek düzeyde güvende tutulması şarttır. [6]

Teknolojik gelişmeler kuşkusuz havacılık navigasyon sistemlerinin doğruluğunu, tutarlılığını, etkinliğini ve sistem sürekliliğini geliştirerek daha iyi çalışmalarını sağlamıştır. Sistem güvenliği, paydaşların havacılık altyapısındaki tehditleri ortadan kaldırmaları sektörde bir zorunluluk haline gelmiştir. Halen, ticari havacılık için siber güvenliği tanımlayan ortak bir vizyon veya ortak strateji, hedefler, standartlar, uygulama modelleri veya uluslararası politikalar bulunmamaktadır. [7] Güvenli bir havacılık sistemi sağlamak ve siber tehditlerin önüne geçmek, hükümetlerin, havayollarının, havaalanlarının ve üreticilerin ortak bir sorumluğudur.

ADS-B, küresel navigasyon sistemini kullanarak uçakların konumlarını bağımsız olarak bulmalarına yardımcı olur. Pilotlar, havadan havaya ve havadan karaya sistemler ile iletişim kuran dijital bir veri bağlantısının yardımıyla yükseklik, hız ve diğer ilgili verileri periyodik olarak iletebilir. Güvenlik bu sistemde önemli bir husustur, çünkü saldırganlar onu kolayca bozabilir ve manipüle edebilir. Sinyali gönderen için

gönderen doğrulama şemasının olmaması ADS-B mesajını alan için güvenlik açığı yaratmaktadır. Bölüm 2'de bu konu detaylı ele alınmıştır. Havacılık navigasyon güvenliği, havacılıkta öngörülen standartlara ve prosedürlere bağlıdır. Bağımlılık, bu standartların sistemin performansı üzerindeki etkisinden kaynaklanmaktadır.

IFF, dost-düşman tanıma sistemi, savaş uçaklarında ve savaş gemilerinde yüklü olan ve uygun radar sinyali ile "sorgulandığında" uçağı veya gemiyi dostça tanımlayan şifreli bir mesajla doğru olarak yanıt veren bir radar transponderıdır. Sorgulayıcı cihazlar arama, gözetleme ve yakalama radarlarına ve ayrıca belirli uçaksavar füzelerinin kılavuz sistemlerine yerleştirilmiştir. IFF ile donatılmış tüm uçaklar ve gemiler, radar tarafından tespit edildiğinde doğru şekilde tepki vermezlerse hedef alınabilirler. Dost-düşman uçakların kimlik tespiti ve erişim kontrolü Hava Savunma Sistemi için gerekli koruma mekanizmalarıdır. Üzerinde anlaşılmış kodlanmış gizli mesajın doğrulanması, yetkisiz erişim için hava alanını düşman uçaklardan korumak için en yaygın ve temel işlemlerden biridir. Bu çalışmada sunulan tanıma yaklaşımı, Hava Savunma Sistemine, hava taşıtı doğrulama ve erişim kontrolü sağlamak için şifreleme şeklinde kodlanmış gizli mesaj alışverişi yapmadan eşzamanlı olarak sağlayabilir.

Bu çalışmanın cevaplamaya çalıştığı temel soru şudur: Uçak filoları arasındaki kimlik doğrulama problemi için nasıl bir çözüm bulabilirim? Bu tez çalışması, uçaklarda yapılan kimlik doğrulamasının güvenliği ile ilgili yapılan araştırmalara genel bir bakış sunar ve yeni bir kimlik tanıma şeması önerir.

2. HAVACILIK SİSTEMLERİ

2.1 Uçuş Kuralları

Uçuş sırasında navigasyon, belirli bir uçuşun görevlerine atanan uçuş kuralları ile belirlenen birçok farklı yöntem ve teknolojiyle gerçekleştirilebilir. Görerek uçuş kuralları (VFR) ve aletli uçuş kuralları (IFR), tüm pilotların izlemesi gereken iki programdır [8].

IFR, dışarıdan görsel referansla yapılan uçuşların güvensiz olduğu koşullar altında uçuşu yönetmek için oluşturulan kurallar ve düzenlemelerdir. IFR veya VFR uçuş planı, pilotlar ve kontrolörler tarafından bir uçağın uçmakta olduğu uçuş planının türünü belirtmek için kullanılan terimlerdir. IFR uçuşu, uçuş güvertesi araçlarına ve navigasyona referansla (elektronik sinyaller referans alınarak) uçar. IFR, tamamen göstergelerde veya ATC kontrolünde navigasyon anlamına gelir.

VFR, bir pilotun uygun hava şartlarında uçağı uçurduğu (genellikle bir pilotun uçağın rota yönünü görebileceği açık bir iklimde) kurallar ve düzenlemelerdir. VFR genellikle ATC'den belirli bir kontrol olmadan uçmak anlamına gelir.

2.2 Havacılık Güvenliği

Havacılık sistemi karmaşıktır, oldukça yenilikçidir ve sürekli değişmektedir. Endüstrinin bu yenilikçi doğası, havacılık topluluğu üyelerinin emniyet ve güvenliği arttırmak için sürekli olarak ortak bir vizyonla birlikte çalıştıkları işbirlikçi bir kültüre ihtiyaç duymaktadır.

Sivil havacılık sistemlerinde artan sayısallaştırma ve otomasyonun geleneksel havacılık güvenliği zihniyetinde bulunmayan yeni güvenlik açıklarına yol açtığını iddia [9] etmişlerdir.

Kablosuz teknolojideki gelişmeler 1990'ların sonunda meydana geldi, yazılım tabanlı radyo (SDR) teknolojisi, bu gelişimin ana itici güçlerinden biriydi. SDR'ler ilk

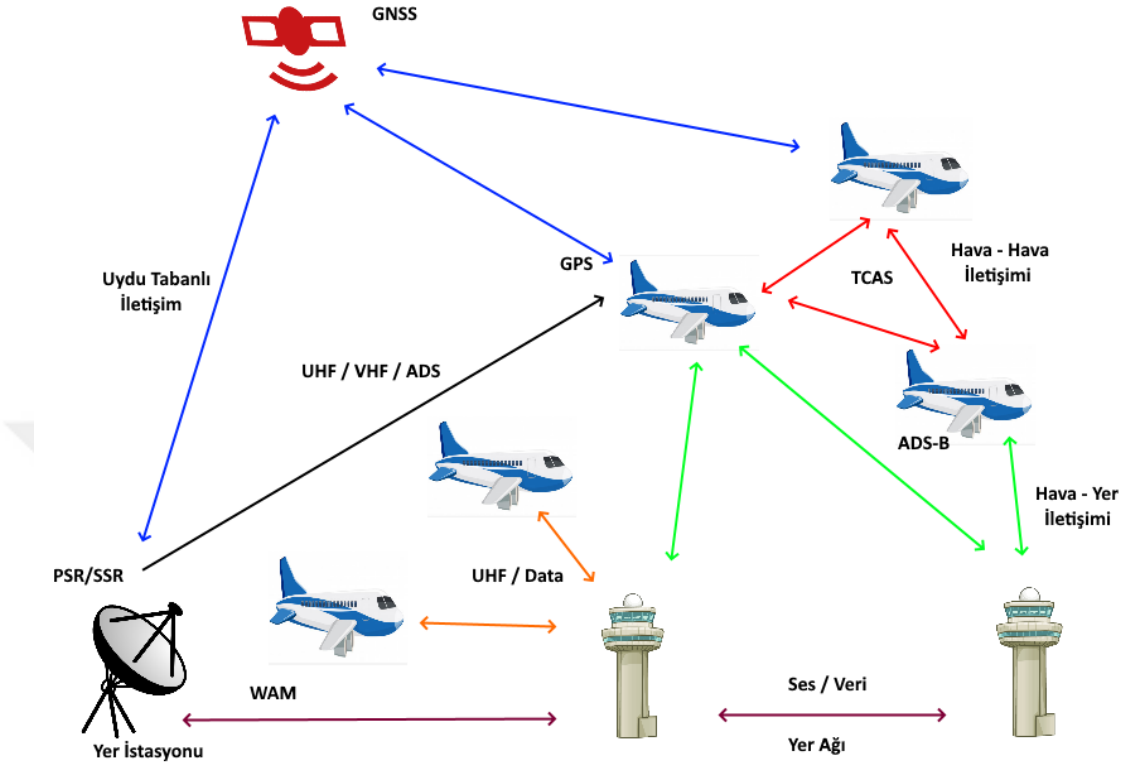
olarak 1990'larda askeri ve kapalı ticari kullanım için geliştirildi, ardından gelişimleri 2001'de piyasaya sürülen GNU Radyosu [10] gibi açık kaynaklı projeler takip etti. Ucuz, ticari kullanıma hazır SDR donanımın mevcudiyeti, geniş bir grup insan için yeni teknolojik imkânlar sağladı. Temel teknoloji bilgisine sahip olan herkes artık havacılık sistemlerinde kullanılanlar gibi isteğe bağlı radyo sinyallerini alabilir, işleyebilir ve iletebilir duruma geldi. Önceden radyo donanımının amaca uygun hale getirilmesi sadece uzmanlar tarafından yapılabilecek masraflı ve karmaşık bir işti, şimdi ise SDR'ler internette kolayca bulunabilen yazılımlar kullanılarak programlanabilir ve sorunsuz bir şekilde uyarlanabilir.

Strohmeier ve arkadaşları [9] havacılıkta, mevcut teknolojideki kimliği doğrulanmamış dijital iletişim ağları kullanarak veri aktarma eğilimi olduğunu gözlemlemişlerdir. Uçuş mesafeleri, uçak pozisyonları veya yolcu bilgileri gibi çeşitli olan bu dijital veriler yerdeki ve uçaktaki otomatik sistemler ile işlenir. Temel protokollerin doğrulanması (authentication) olmadan, veri bağlantısı (data link) seviyesindeki saldırıların, hem havacılık sistemleri hem de bu sistemlerin kullanıcıları için tespit edilebilmesi, ses haberleşme sistemi veya birincil gözetim radarı (PSR) gibi geleneksel analog teknolojilere yapılan saldırılardan daha zordur.

2.3 Hava Trafik Kontrolü

ATC'nin hava sahasını güvenli bir şekilde yönetebilmesi için, her kontrol biriminin kontrol altındaki her bir uçağın durumunu anlaması gerekir. Geleneksel olarak, Birincil Gözetim Radarı (PSR) ve İkincil Gözetim Radarı (SSR) çeşitli şekillerde II. Dünya Savaşı'ndan bu yana bu rolü yerine getirmiştir. Her iki sistem de, radyo iletiminin büyük bir finansal yatırım ve uzmanlık gerektirdiği bir zamanda tasarlanmıştır. Bu nedenle, bu eski sistemlerde güvenlik açığı düşünülmemiş, çünkü erişilemeyecekleri varsayılmıştır. Yazılım Tabanlı Radyo (SDR)'nun yükselişi, bu varsayımı geçersiz kılmış ve potansiyel saldırganlara çok daha az kaynak ile saldırma olanağı vermiştir [11]. Tek Avrupa Seması ATM Araştırma Programı (SESAR) ve Amerikan NextGen programları gibi havacılık araştırma programları ile birçok yeni hava trafik kontrolü ve iletişim protokolü yayınlanmaktadır. Gözetim ve birlikte çalışabilirlik sunan temel ATM sistemleri : Birincil ve İkincil Gözetim Radarı,

Otomatik Bağımlı Gözetim-Yayını, Trafik Çarpışma Kaçınma Sistemi ve Geniş Alan Multilateration. Bu sistemlerin birbirleriyle etkileşimleri Şekil 2.1 ‘de gösterilmiştir.



Şekil 2.1 : ATM cihazları etkileşimi.

Hava Trafik Yönetimi’nin gözetim sistemleri hakkında özet bilgi Çizelge 2.1 ’de gösterilmiştir.

2.4 Aviyonik Sistemler

Yeni nesil bilgisayarlar, iletişim donanımı, yazılım dilleri ve geliştirme araçlarının hızlı bir şekilde gelişmesiyle kendi başına bir disiplin olarak görülen teknik alanlardan biri, aviyoniktir. Aviyonik genişledi ve “multidisipliner bir disiplin” haline geldi.

“Avionics” havacılık elektroniği demektir. Bir uçakta kullanılan bütün elektronik sistemleri kapsar. Bu sistemler temel olarak navigasyon, haberleşme, gösterge ve diğer uçuş ve görev fonksiyonlarını yerine getirir. İlk defa 1930’larda telaffuz edilmeye başlanılmış, II.Dünya Savaşı ve sonrasındaki soğuk savaş yıllarında bilimsel ve teknolojik olarak büyük gelişmeler katetmiştir. Askeri aviyonik sistemler insanlı,

Çizelge 2.1 : ATM sistemlerinin temel özellikleri, bağımlılıkları ve açıkları.

Sistem	Yer/Hava Bağımlı	Statü	Teknoloji	Bağımlılık	Zafiyet
PSR	Yer	Kullanımda	Tespit edilen radyo sinyali yansımalarını kullanarak hedeflerin yönünü ve mesafesini ölçer	Uçak hedefinden bağımsız	Bilişim teknolojileri IT) ile ilgili değil.
SSR	Yer	Kullanımda	Kimlik, irtifa, hız gibi uçaklardan ek bilgi talep eder	Transponder ile donatılmış hedefler	Gizli dinleme
TCAS	Hava	Kullanımda/ 2015 yılından beri zorunlu	Hedef kimlik sorgulaması	Transponder ile donatılmış hedefler	Gizli dinleme, karıştırma (yayın telsiz),yanıltma sinyali
ADS-B	Hava	2020'ye kadar uygulanması şart koşulmuştur	Kimlik, irtifa, hız hakkında bilgi yayınlayan hedefler	Transponder ile donatılmış hedefler	Gizli dinleme, karıştırma (yayın telsiz),yanıltma sinyali
WAM	Yer	Yayılma aşamasında	ADS'i, sağlamlık için PSR ve SSR verileriyle birleştirir	Merkezi İşlem BT tabanlı bilgiler	Veri işleme ve BT ile ilgili

insansız uçakların, füzelerin ve silahların vazgeçilmezidir. Bu sistemler uçağın savunma, saldırı ve gözetleme görevlerini yerine getirmesini sağlar [12].

2.4.1 Aviyonik yazılım standartları

Aviyonik yazılımı, aviyonikte kullanılan yasal olarak zorunlu güvenlik ve güvenilirlik endişelerine sahip gömülü bir yazılımdır. Aviyonik yazılımı ile konvansiyonel gömülü yazılımların arasındaki temel fark, güvenlik için optimize edilmiş olması ve geliştirme sürecini gerektiren yasal düzenlemelerdir. Güvenliği ve güvenilirliği sağlamak için FAA(Federal Havacılık İdaresi), CAA(Sivil Havacılık Otoritesi), DoD(Amerika Birleşik Devletleri Savunma Bakanlığı) gibi ulusal düzenleyici otoriteler yazılım

geliştirme standartlarına ihtiyaç duyar. Aviyonik geliştirmeye etkisi olan bazı standartlar : MIL-STD-498,RCTA DO-178B, ISO 15288, ANSI/EIA-632, APR 475.

DO-178B

D0-178B havadaki sistemlerde kullanılan güvenlik açısından emniyet kritik yazılımların geliştirilmesiyle ile ilgili bir kılavuzdur. RTCA ve EUROCAE ile ortak geliştirilmiştir. Kurallar zamanla deneme-yanılma ile geliştirilmiştir. Bu kavram ilk olarak DO-178 tarafından tanıtıldı, yazılımın güvenlik kritikliğine (Çizelge 2.2) bağlı olan yazılım doğrulama gereksinimleri tanımlandı. Yazılım uygulamaları üç kategoriye ayrılmıştır: kritik, zorunlu ve gerekli olmayan.

DO-178B'de amaç, güvenliğe yönelik bir güven derecesiyle amaçlanan işlevleri yerine getiren ve uçuş güvenliği gerekliliklerine uyan havada çalışan sistemler için ayrıntılı yazılım yönergeleri sağlamaktı.Tüm aviyonik sistemler aynı kritikliğe sahip değildir. Bazı sistemlerin arızaları güvenliği etkilemeyebileceğinden çok sıkı bir geliştirme sürecinin izlenmesini gerektirmeyebilir. Bunun için, DO-178B farklı arıza durumu kategorilerini içerir. Yazılımın kritiklik seviyesi, yazılımın sistem güvenliği değerlendirme süreci tarafından belirlenen olası arıza koşullarına etkisine dayanır. Yazılım emniyet seviyeleri A, B, C, D, E 'dir, Çizelge 2.2'de bu seviyelerin tanımlamaları yer almaktadır.

2.4.2 Askeri aviyonik sistemler

Askeri aviyonik sistemler uçağın tipine, üretim veya modernizasyon tarihine bağlı olarak farklı şekillerde sınıflandırılabilmektedir. Günümüz modern uçaklarının yapısına bağlı yapılacak bir sınıflandırma aşağıdaki gibidir [12]:

1. Navigation: Seyrüsefer sistemleri.
2. Communications: Haberleşme sistemleri.
3. Sensörler.
4. Mission System: Görev kontrol sistemleri.
5. Göstergeler ve kontrolleri.

Çizelge 2.2 : DO-178B Yazılım emniyet seviyeleri tanımları.

Emniyet Seviyesi	**Hata Sınıfı İsim-lendirmesi**	**Hata Tanımı**	**Başarısızlık olasılığı (uçuş saati başına)**
A	Catastropic (Ölümcül)	Güvenli uçuş ve inişin devam etmesini önleyen koşullar, uçağı düşürebilecek koşullar	10^{-9} 'dan az
B	Hazardous (Tehlikeli)	Tehlikeli veya ciddi bir arıza durumuna neden olabilecek veya katkıda bulunabilecek yazılım-lar. Ölümcül yaralan-malara sebep olabile-cek durumlar	10^{-7} ve 10^{-9} arası
C	Major (Büyük)	Uçak güvenliğini önemli ölçüde azaltan koşullar, mürettebatın olumsuz koşullarda çalışması	10^{-5} ve 10^{-7} arası
D	Minor (Küçük)	Uçak güvenliğini önemli ölçüde azaltmayacak koşullar, mürettebat iş yükünde hafif artış olması	10^{-5}'den büyük
E	No Effect (Etkisiz)	Uçağın çalışmasını veya mürettebatın iş yükünü etkilemeyen koşullar	-

2.4.3 Haberleşme, navigasyon ve tanıma-tanıtma sistemleri

Tüm askeri uçaklar görevlerini tamamlayabilmek için görev sensörleri ve silahlarından ayrı olarak belli hesaplama yeteneklerine ve hesaplama kaynaklarına ihtiyaç duyar [13]. Bunlar:

1. Haberleşme (Communications): Dost kuvvetlerle, aynı uçaktaki personelle, filodaki diğer uçaklarla, yerdeki komuta kontrol merkezi veya karadaki askerlerle ses veya veri olarak iletişim kurma yeteneği.

2. Navigasyon(Seyrüsefer-Navigation): Askeri platformun görev gereği bir hedefe, ara noktalara, randevu noktasına, başlangıç noktasına yeterli doğrulukla gide-bilmesini sağlayan sistemler.

3. Tanıma - Tanıtma (Identification): Verilen bir hedefe nişan alma kuralları. Ateş etmeden önce hedefi sınıflandırma ve tanımlama yeteneği.

Bu üç sistem, askeri uçaklarda CNI (Communication, Navigation, Identification) olarak tanımlanmaktadır.

1. Dost Düşman Tanıma Tanıtma Sistemi (IFF).
2. Hava Trafik Kontrol (ATC) Mode S.
3. TCAS.

2.4.3.1 Dost-düşman tanıma sistemleri (IFF-Identification Friend or Foe)

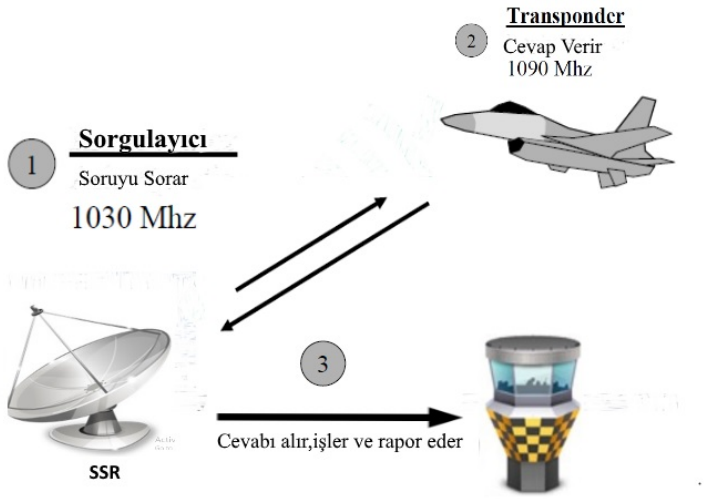
II. Dünya Savaşı sırasında, radarın gelişimiyle, görsel menzilin ötesinde dost uçakların belirlenmesi yeteneğine sahip sistemler geliştirmek gerekli oldu. IFF sisteminden gelen bilgiler karar yardım sürecinin bir parçasını oluşturur, silah ateşlenmenden önce ve dost olmayan hedefe karşı harekete geçilmeden önce bu sistemden gelen bilgiler değerlendirilmelidir. IFF sistemleri gemi, uçak veya helikopter gibi platformları tanıma tekniğidir. Hem sivil hem de askeri dünyada yaygın olarak kullanılmaktadır.

Eski sistemler, dost uçaklar tarafından yayınlanan düzenli bir sinyalin üçgenleştirilmesine dayanıyordu. Daha sonrasında, transponder(alıcı verici cihaz) olarak çalışan ve birincil radar darbesine yanıt olarak çok yönlü(omnidirectional) yükseltilmiş darbe gönderen gelişmiş bir sistem geliştirildi. Böylece, bu ilk transponderlara sahip dost uçak, aynı radar ekranındaki diğer ekolardan daha parlak bir şekilde parladı. SSR(ikincil gözetim radarı) şu anda askeri ve sivil hava trafik kontrol sistemlerinde kullanılmaktadır. SSR'nin askeri kullanımı IFF olarak bilinir [14]. SSR'de amaç, hedefin varlığını saptamak ya da birincil radarda olduğu gibi konumunu tam olarak belirlemek değil, hedefi kesin olarak tanımlamak ve onu diğerlerinden ayırmaktır. Birincil ve ikincil gözetim radarları sıklıkla birlikte kullanılır ve çoğu durumda antenleri aynı anda döner [15].

Modern IFF sistemleri hala bir sorgulama sisteminden gelen bazı uyaranlara cevap olarak çok yönlü bir iletim (omnidirectional transmission) gönderen bir transponder temelinde çalışmaktadır.

Bu sistemler, sorgulama sisteminin transponderlara farklı "sorular" sorma ve transponderların cevap içinde kodlanmış bilgilerle cevap vermelerini istemektedir. Sorgulama sistemi genellikle dinleyen transponderlardan, irtifalarını veya kimlik kodu numaralarını bildirmelerini ister.

Modern sistemler hala ilk IFF sistemlerinde olduğu gibi dostane hedeflerin işbirliğine dayanmaktadır. Dost hedef uygun bir transponder taşımalı ve bu transponder çalışır durumda olmalıdır. Ayrıca, bir IFF yanıtının eksikliği hedefin mutlaka bir düşman olduğu anlamına gelmez; sadece transponderı olmayan dost uçak olabilir. Bu nedenle, ismine rağmen, IFF sistemleri dost hedefleri tanımlamak için kullanılabilirler, düşman hedefleri belirleyemezler. Potansiyel düşman hedefleri tespit etmek için, birincil radar (PSR) hala gereklidir [16]. Modern IFF sistemleri dost tanımasına ek olarak filo, yan numara(kuyruk kodu), irtifa bilgisi gibi uçağa ait diğer bilgileri de sağlar. Şekil 2.2'de temel IFF sistemi çalışma mantığı gösterilmiştir.



Şekil 2.2 : Temel IFF sistemi çalışma adımları.

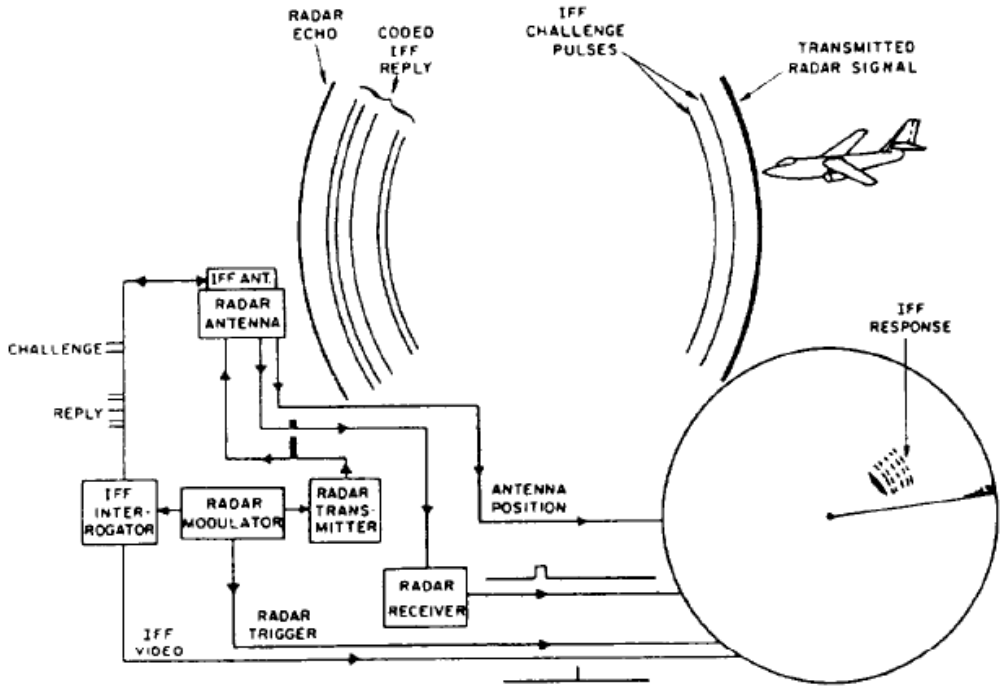
IFF, kimlik tanımlama sürecini üç temel adımda tamamlar [1] :

1. **Kimlik sorma** : IFF sorgulayıcısı şifrelenmiş kimlik sorgusunu darbe çiftleri arasında gönderir. Seçilen çalışma modu darbeler arasındaki mesafeyi belirler.

2. **Cevaplama**: Dost hedefin IFF aktarıcısı, şifrelenmiş kimlik sorusuna çok yönlü iletimle (omnidirectional transmission) otomatik olarak cevap verir. Sorgulayıcının

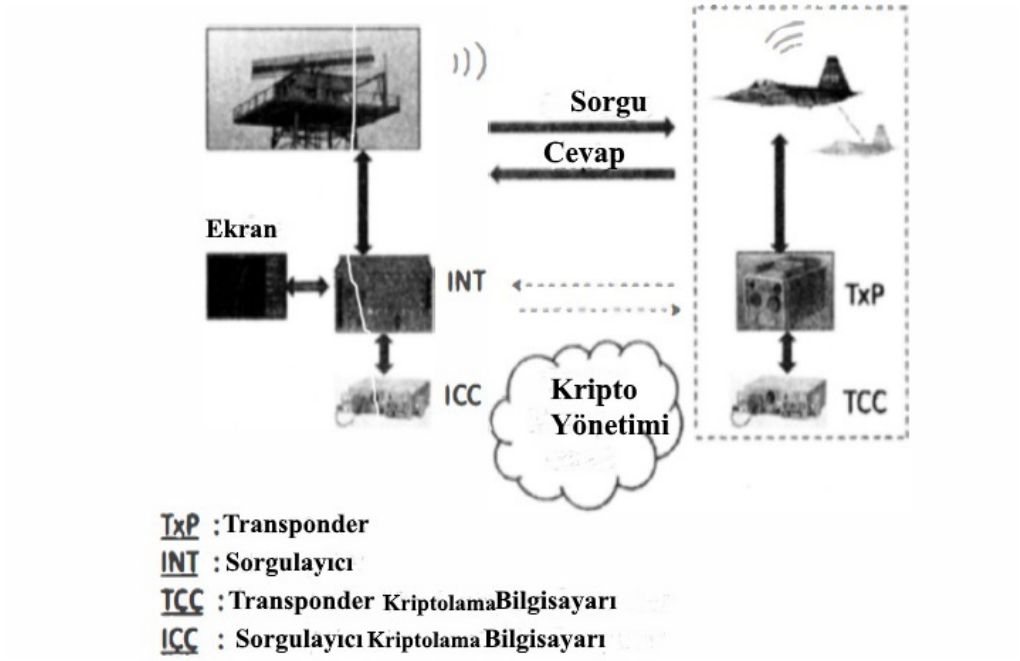
(interrogator) frekansından biraz farklı bir frekansta farklı bir darbe seti gönderir. Bir bastırma (blanking) sinyali, uçağın transponderının kendi sorgulayıcısına cevap vermesini önler.

3. **Tanıma** : IFF sorgulayıcısı şifrelenmiş cevabı alır ve bir göstergede gösterilmek üzere işleme koyar. Hedefin tanınması, PPI (Plan durum göstergesi) göstergesine dayanır. Dost uçaktan gelen şifrelenmiş cevap normalde Şekil 2.3'de gösterildiği gibi hedef eko sinyalinin hemen ötesinde kesikli bir çizgi olarak görünür.



Şekil 2.3 : IFF operasyonunun temelleri [1].

Askeri eğitim veya çatışma sırasında, sorgulayıcıya ve alıcı-vericiye (Transponder-TxP) bağlı Kriptolama Bilgisayarları (CC) kullanarak dost hedefleri tanımlamak için güvenli bir IFF modu kullanılır. Sorgulayıcı Kriptolama Bilgisayarı (ICC) tipik olarak şifreli sorgulama darbeleri üretir ve dost platform sorgulamanın şifresini başarıyla çözdüyse, sorgulayıcıya ne zaman cevap bekleneceğini bildirir. TxP şifreli bir sorgu aldığında, bunu Transponder Kriptolama Bilgisayarı (TCC)' na geçirir ve TCC sorgulamayı başarıyla çözerse, cevabı ne zaman üreteceğini TxP'ye bildirir (Şekil 2.4). SSR/lFF'in teknik özellikleri, NATO tarafından oluşturulan STANAG-4193 belgesi olarak bilinen bir Standardizasyon Anlaşması ile yönetilmektedir [17].



Şekil 2.4 : ICC ve TCC [2].

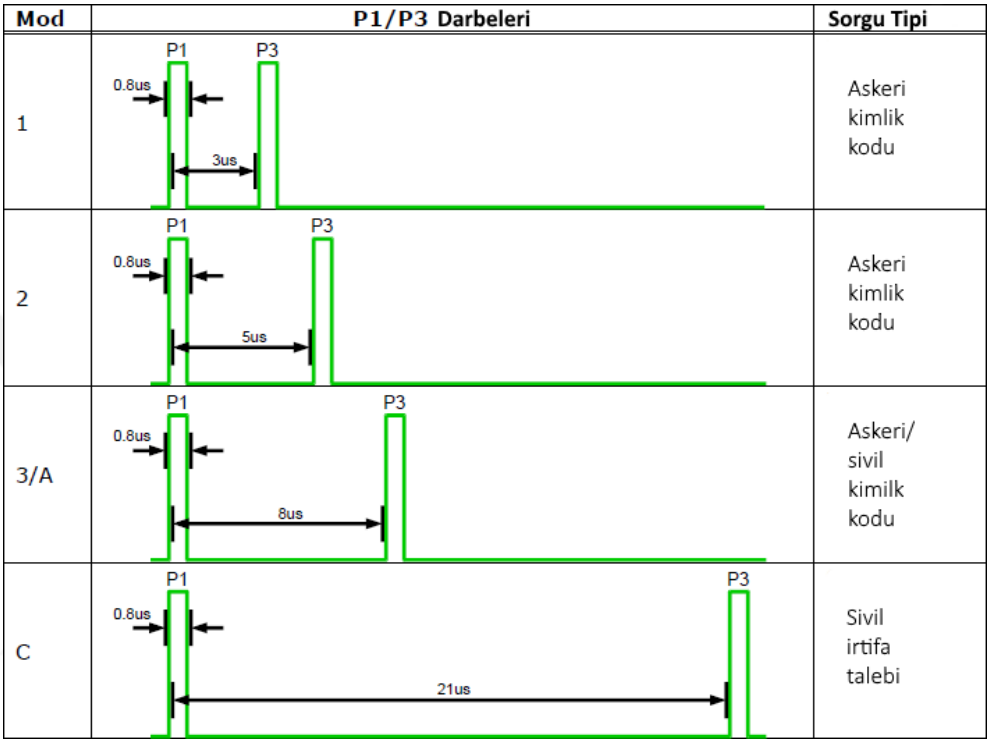
AIMS MARK XII IFF Sistem

AIMS, hava trafik kontrol radar işaret sistemi (ATCRBS), dost-düşman tanıma sistemi (IFF), Mark XII sisteminin kısaltmasıdır. ATCRBS, dünya çapında hava trafik kontrolü için kullanılan sivil hava trafik kontrol sistemidir. IFF askeri sistemleri tanımalar. AIMS sistemi sorgulayıcılar, alıcı-verici cihazlar (transponders), sorgulama yolunda yan lobların bastırılması (ISLS) anahtarları ve sürücüleri , defruiters (mevcut meyve "Fruit" parazitlerinin optimizasyonu için "Defruiter" adı verilen bir aygıt kullanılır), çözücüler (decoders), kripto bilgisayarlar gibi ekipmanlar içerir.

Operasyon modları

Şu anda SSR/IFF' de yaygın olarak kullanılan yedi çalışma modu vardır. Bu modların isimleri 1, 2, 3/A (kimlik tespiti cevabı), C (uçak irtifası cevabı), 4, 5 ve S 'dir. Askeri platformlar genel olarak 1, 2, 3, 4 ve 5 modlarını kullanırken, sivil platformlar genellikle A, C ve S modlarını kullanır. Mod 1, 2 ve 3, Seçici Kimlik Tanıma Özelliği(SIF) modları olarak bilinir. Dünyadaki birçok ülke hala sadece SIF modlarını kullanmasına rağmen, S Modu şu anda SIF modlarının yerine kullanılıyor [2].

Modern bir IFF kurulumunda, sorgulama sistemi iki darbe şeklinde kodlanmış bir sorgu gönderir (P1 ve P3) ve dost uçaktaki transponder cevap döner, kendisi hakkında bilgiler verir. Sorgu darbeleri P1 ve P3 arasındaki süre havadaki transpondere hangi bilginin istendiğini söyler. Şekil 2.5'te en yaygın askeri ve sivil IFF sorguları için P1/P3 darbe modelleri gösterilmektedir.



Şekil 2.5 : SIF Modları.

SIF modları

Dost uçaklar için hava trafik kontrolü ve kod izleme, seçici kimlik tanıma özelliği (SIF) modlarını (mod 1, 2 ve 3 / A) kullanır. Bu modlardaki yüklemeler , her darbe için özel aralıklar koyulmuş iki darbe içerir. ISLS işlemi için 3. darbe gerekir.

Mod 1: Sadece askeri kullanım içindir. Cevap kodunun ilk basamağı, 0 ila 7 arasında bir sayı olmalıdır. İkinci basamağı 0-3 arasında bir sayı olmalıdır. Kalan iki hane normalde 0 olacaktır. Uçak tipini veya görevini tanımlayan "görev kodu" içerir.

Mod 2: Transponder ünitesinde ayarlanan Mod 2 işlemi de sadece askeri kullanım içindir. Uçağın kuyruk numarasını belirtir. Mod 2 ve 3 / A cevap kodlarında, dört cevap hanesinden her biri 0 ila 7 arasında herhangi bir değere sahip olabilir. Uçuş sırasında genellikle değiştirilemez.

Mod 3/A: Standart hava trafik kontrol modudur. Otomatik irtifa raporlama modu (C Modu) ile birlikte uluslararası olarak kullanılır. Askeri veya sivil kullanım için uygundur. Askeri acil durum cevapları, 4X ve 7700 kodlarının birleşiminden oluşur. Sivil acil durum raporları sadece 7700 kodunu kullanıyor.

7600 cevap kodu: Hem askeri hem de sivil kullanım için uygun, telsiz iletişimindeki bir başarısızlığa işaret ediyor.

7777 cevap kodu: Aktif hava savunma misyonlarındaki önleyicilerine atanır.

Mod C: Sivil ve askeri uçaklar tarafından kullanılan C Modu yanıtları, uçakların irtifalarını gösterir ve otomatik olarak hava aracının barometrik altimetresinden alınır.

Mod 4 ve Mode 5

Mod 4 ve Mod 5'in tarihçesine bakacak olursak 1970'de Mode-4, askeri kripto iletişimi NATO ülkeleri tarafından uygulandı. 1990'larda Mode-4 eksiklikleri tespit edildi ve Mode-5'in tanımı ve uygulaması başladı. 2000'de Mode 5 NATO ülkeleri tarafından tanımlandı ve kabul edildi. Mod 5'in iki farklı seviyesi vardır: Seviye 1, hem GPS hem de geleneksel araçlara dayalı zaman, konum ve tanımlama sağlayan sorgu yanıt modudur. Seviye 2, yayın modudur ve tamamen GPS'i temel alır. NATO-STANAG 4193 Bölüm I'de Mod 4, NATO-STANAG 4193 Bölüm V'de Mod 5 açıklanmıştır. Mod 5'in bazı avantajları:

- Mevcut çalışma modlarındaki (1, 2, 3 / A, C, 4) performans ve güvenlik sorunlarını gidermek için modern modülasyon, kodlama ve şifreleme tekniklerini kullanır.
- GPS konumunun ve ADS-B gibi diğer genişletilmiş verilerin geçilmesi için genişletilmiş veri işleme yeteneğine sahiptir.
- Mevcut Hava Trafik Kontrolü (ATC) sistemleriyle uyumludur.
- Time-of-Day kimlik doğrulaması ile güvenlik özellikleri eklenilmiştir, yeni şifreleme algoritması kullanmaktadır.

2.4.3.2 MOD S

Sivil uçaklar artan sayı ve hızlarıyla hava trafik denetiminde sorunlar yaratabilmektedirler. Bu sorunların üstesinden gelebilmek için, dünya çapındaki sivil kuruluşlar IFF teknolojisini sivil hava trafik kontrol ortamlarına uyarlamışlardır. Bu ortamlarda

IFF sistemi, SSR (Secondary Surveillance Radar) olarak adlandırılmaktadır. Mod S (Selective), yoğun trafik ortamlarında Hava Trafik Kontrol sistemlerini (ATC) desteklemek için kullanılan bir gözetleme (Surveillance) ve veri linki sistemi olarak geliştirilmiştir. Sistemin kendi kendine parazitini azaltmak için adresli bir sorgulama modudur Mod S. Sistemin Sivil havacılıktaki uygulama şekilleri Uluslararası Sivil Havacılık Teşkilatı (ICAO) tarafından, ICAO Annex 10 (Volume III ve IV) dokümanlarında tanımlanmaktadır. Mod S sistemi ile adresli sorgulama yeteneği, veri linki kabiliyeti ile uçağa ait uçuş bilgisi, hız, güzergâh, hava durumu gibi bilgilerin aktarılabilmesi mümkündür. Bu sayede hava trafik kontrolü daha etkin yapılabilmektedir. Mod S, her bir uçağa atanan 24-bit adrese göre uçağın seçici olarak sorgulanmasını sağlayan İkincil Gözetim Radarı'dır. Mod S'te uçaklar kendilerine bir sorgulama yapılmadan dahi, kimlik ve uçuş durumları hakkındaki bilgileri periyodik olarak yayınlayabilirler (Automatic Dependent Survaillance - Broadcast, ADS-B). Bu sayede daha iyi bir trafik kontrolü ve daha az elektromanyetik kirlenme sağlanabilmiştir [18].

Mode S sisteminin temel amaçlarından biri, eski Mode A/C veya ATCRBS (Hava Trafik Kontrol Radar Beacon Sistemi) ile ilgili operasyonel problemleri çözmektir [19].

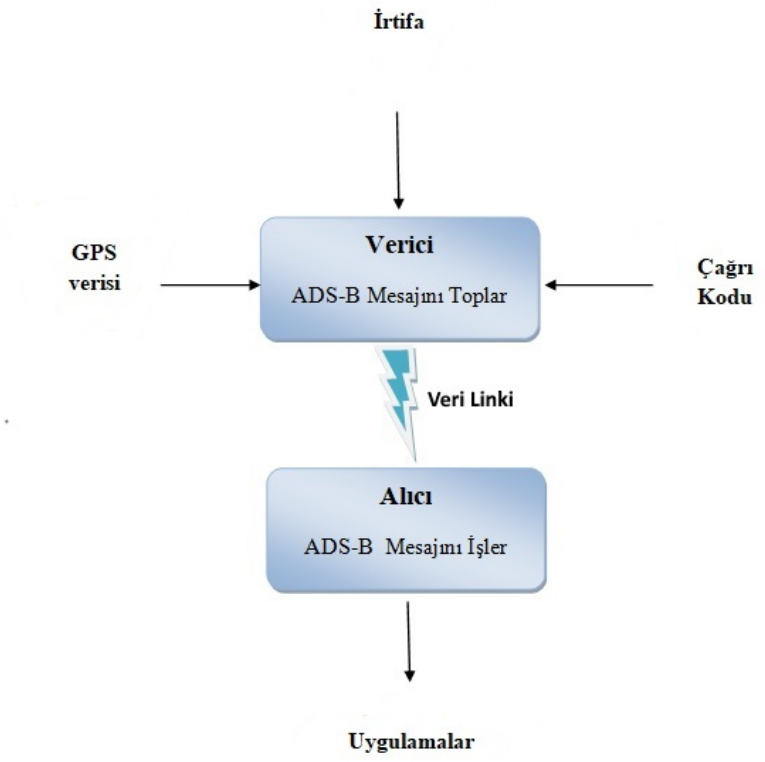
2.4.3.3 Otomatik Bağımlı Gözetim Yayını (ADS-B)

Hava yolculuğuna olan talep giderek artmaktadır. II. Dünya Savaşı teknolojisini kullanan hava trafik kontrol sistemleri değişmeden kalırken, artan trafikle başa çıkmaları zorlaşmıştır. Yüksek trafik yükü altında çalışmak ve modern teknolojiyi benimsemek için, Federal Havacılık İdaresi (FAA), 2012'de Yeni Nesil Hava Taşımacılığı Sistemini (NextGen) uygulamaya koymuştur. Otomatik Bağımlı Gözetleme Yayını (ADS-B), güvenlik gözetimi nedeniyle dikkat çeken bu NextGen programının bir yönüdür. ADS-B teknolojisinde veri doğrulaması veya gönderici doğrulama şeması bulunmayan güvensiz bir veri bağlantısı üzerinden bir yayın sinyalinin kullanılması, uçak sahtekârlığı, mesaj değişikliği ve mesaj yerleştirme saldırıları için açık bir kapı bırakmaktadır [20]. Bu çalışmada önerilen tanıma şeması ADS-B'deki gönderici doğrulama eksikliğini giderebilir.

ADS-B, hava trafik kontrolü için tamamen yeni bir paradigmadır. Her katılımcı, yerleşik bir GPS alıcısı kullanarak kendi konumunu ve hızını alır. Konum daha sonra periyodik olarak bir mesajda (tipik olarak saniyede iki kez) ADS-B Out adı verilen verici alt sistem tarafından yayınlanır. Mesajlar daha sonra, alıcı alt sistem ADS-B In ile donatılmışsa, yerdeki ATC istasyonları tarafından ve yakındaki uçaklar tarafından alınır ve işlenir.

ADS-B fonksiyonu geleneksel Mode S transponderlarına entegre edilebilir.

Sistem, ADS-B mesajları üreten uçaktaki bir vericiden, veri linki yayın ortamından ve başka bir uçaktaki, araçtaki, yer sistemindeki mesajları işleyip görüntüleyen alıcıdan oluşur. Şekil 2.6'de ADS-B mesaj akışı gösterilmiştir.



Şekil 2.6 : ADS-B mesaj akışının gösterilmesi.

ADS-B harflerinin anlamları:

Otomatik: Uçak ve yer bazlı ADS-B donanımı, ADS-B bilgilerini otomatik olarak yayınlar.

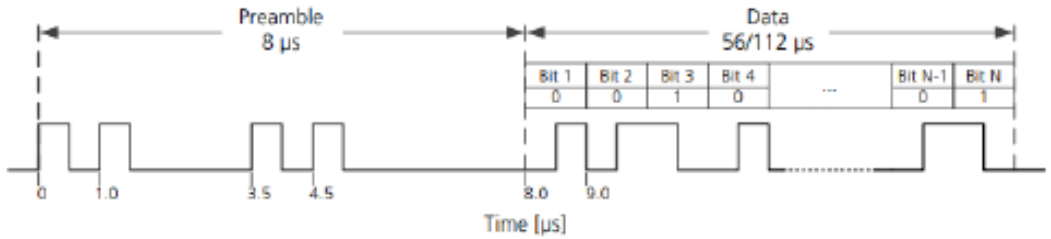
Bağımlı: ADS-B, konum verileri için uçuş yönetim sisteminde olan GNSS sinyallerine bağlıdır.

Gözetim: ADS-B uçağı ve ATC için benzeri görülmemiş bir hava trafiği farkındalığı.

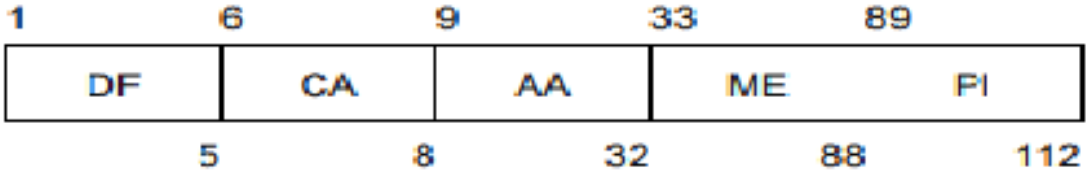
Yayın: ADS-B , ADS-B'yi almak için donatılmış yer istasyonuna ve uçaklara düzenli olarak navigasyon verilerini ve diğer uçuş bilgilerini sürekli yayın yapar.

ADS-B mesajı

Bir ADS-B / Mode-S sinyali her zaman iki bölümden oluşur: 8 μs uzunluğunda bir başlangıç ve bir veri bloğu. Veri bloğu 56 veya 112 darbe zaman dilimi uzunluğundadır. Tüm darbelerin süresi 1 μs'dir (Şekil 2.7). ADS-B yayını herhangi bir sorgulayıcı olmadan yayın yapar. DF17 data formatındadır (Şekil 2.8).

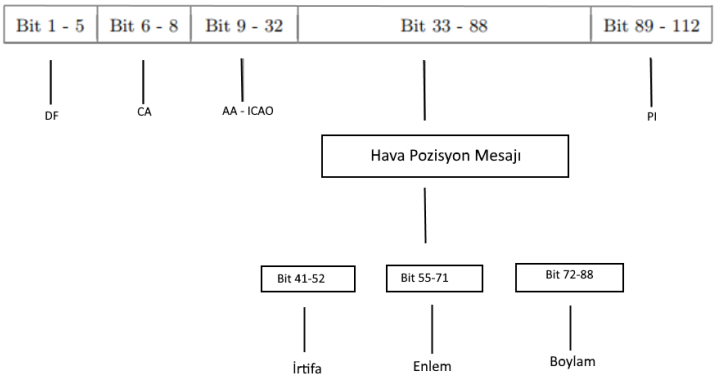


Şekil 2.7 : Mode-S / ADS-B haberleşmesinin darbe konum modülasyonu kullanan sinyal yapısı [3].

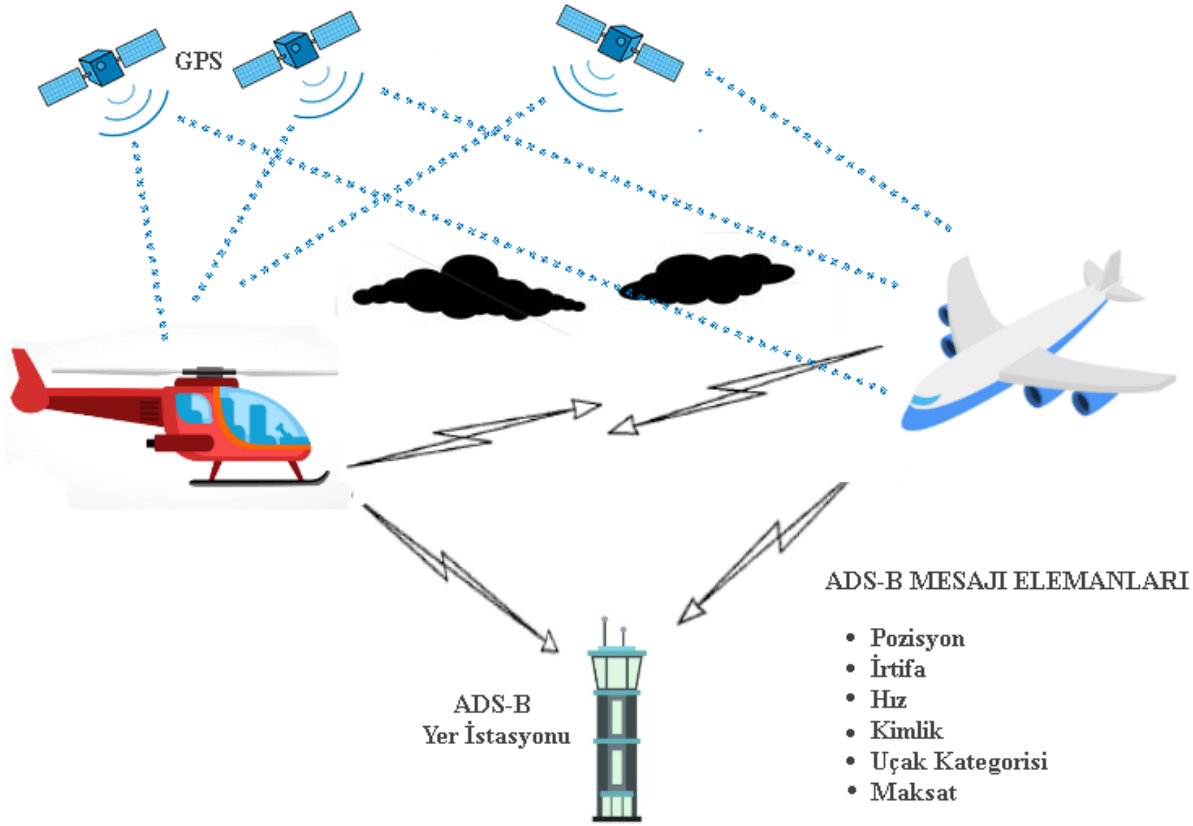


Şekil 2.8 : Extended Squitter, Dowlink Format 17.

Veri paketi (56 μs ve 112 μs uzun veri blokları için geçerlidir) 5 bit downlink formatı (DF) bilgisi ile başlar. Bu formatların bazıları askeri amaçlar için ayrılmıştır. Hava Pozisyon Mesajını (APM) içeren ADS-B 1090ES (Extended Squitter) format numarası DF17'dir (Şekil 2.9). Farklı mesaj içerikleri de olabilir Şekil 2.10'deki gibi. Aşağıdaki açıklama yalnızca DF17 için geçerlidir ve diğer downlink formatları için farklı olabilir. DF alanını 3 bitlik bir CA (kabiliyet) alanı takip eder. Uçağın ICAO adresi 24 bit uzunluğunda AA (uçak adresi) alanı kullanılarak iletilir. Extended squitter için mesaj alanı 56 bit uzunluğundadır ve enlem, boylam ve yükseklik bilgileri içerir. 1090 MHz Extended Squitter 56 bit adrese ek 56 bit pozisyon bilgisinin eklenmesiyle oluşmuştur. Extended Squitter, Mode S transponder da denilebilir. Son alan, hata ayıklaması için 24 bitlik parity bilgisi (PI) alanıdır [3].



Şekil 2.9 : DF17'nin mesaj yapısı.



Şekil 2.10 : ADS-B mesaj içerikleri.

ADS-B güvenlik problemleri

ADS-B ile ilgili güvenlik problemleri arasında, uçağın gökyüzündeki kimliğinin doğrulanmaması bulunmaktadır. FAA, ADS-B'nin gizlilik ve kimlik doğrulamadaki güvenlik zayıflıklarını doğrudan onaylamıştır [21]. Mevcut yer temelli gözetim sisteminden uydu tabanlı bir ADS-B sistemine geçiş, bu tür bir sistemin kötü niyetli düşman için sağlayacağı fırsatları dikkatlice ve titizlikle inceleyerek yapılmalıdır.

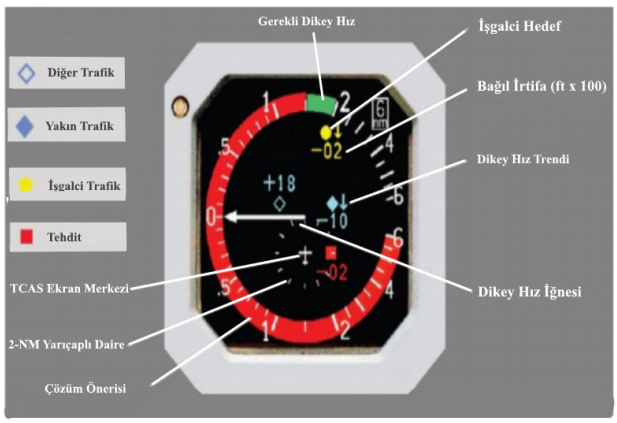
2.4.3.4 Trafik Çarpışma Kaçınma Sistemi (TCAS)

Trafik çarpışmadan kaçınma sistemleri uçağın yakınındaki uçakların yön, menzil ve yüksekliğini gösterir ve çarpışma tehlikesi yaratmaları durumunda pilotu uyarır. Bu işlemi yapabilmesi için diğer uçakların da TCAS cihazına (Şekil 2.11) sahip olmaları gerekir. TCAS, sorgulama sinyallerini diğer ATC transponder donanımlı uçaklara iletir ve diğer ATC transponder donanımlı uçaklardan yanıt sinyalleri alır.

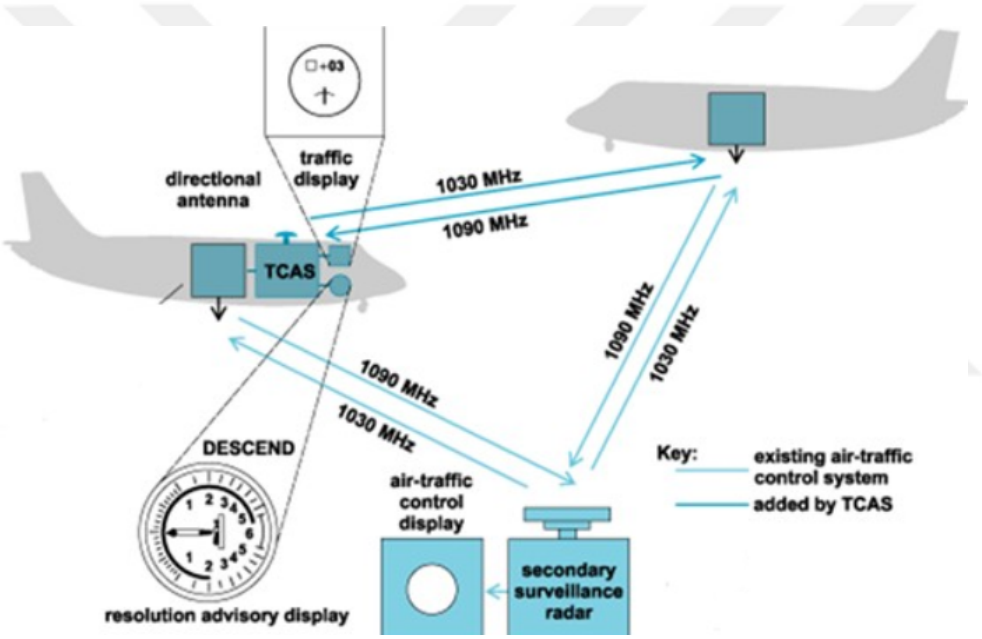
TCAS, İkincil Gözetim Radarı (SSR) ile benzer şekilde çalışır, fakat havadan havaya rol oynar (Şekil 2.12).

TCAS ve ADS-B karşılaştırması [22]:

- TCAS bir çarpışma önleme sistemidir, hedef uçağın korumalı alana girip girmediğini tahmin etmek için, TCAS, ATC transponderini sorgular ve cevap sinyalini alır. ADS-B, bilgilerini sorgulamadan otomatik olarak yayınlar.
- TCAS, çakışmayı sadece şu andaki ve geçmişteki konum ve hıza dayanarak hesaplar; trafik akışı arttıkça çatışmayı tahmin etme yeteneği karmaşıklaşır. ADS-B, doğrudan diğer uçaklardan pozisyon ve hız alır, böylece diğer uçakların rotasını hesaplamak kolaydır.
- TCAS, 1030 MHz frekansındaki ATC transponderını sorgular ve 1090 MHz frekansında cevap veren ATC transponderının cevabını alır. ADS-B, bilgilerini 1090 MHz frekansında yayınlar. Böylece, TCAS, ATC transponderının yanıtlama sinyalini ve ayrıca ADS-B yayın sinyalini alabilir.



Şekil 2.11 : Klasik TCAS göstergesi.



Şekil 2.12 : TCAS çalışma şekli [4].

3. LİTERATÜR ÇALIŞMALARI

Dost düşman tanıma sistemlerinin (IFF) kritik bir öneminin olması, bu soruna dair birçok çalışma yapılmasına sebebiyet vermiştir.

Roger Voles [23] temel kimlik saptama kodlarının sorgulayıcı(interrogator) ve cevaplayıcı(responder) arasında iletildiği bir dost düşman tanıma sistemi önermiştir. Sistemde paylaşılacak kodlar zamanla beraber, sorgulayıcı ya da cevaplayıcının sorgulama zamanındaki pozisyonuna da bağlıdır ve bunlara göre seçilir. Sistemin bir versiyonunda, kodun kullanım ömrü, ilgili sorgulayan ya da cevaplayan aralığındaki yayılma süresi en büyük olana eşit veya daha küçüktür. Etkileşimli sorgulama, temel kodlarla aynı tarzda seçilen başka kodlar kullanılarak da yapılabilir. Sorgulayıcı ve verici arasındaki lokal bilgi de iletilebilir. Bu operasyonları gerçekleştirmek için kullanılan bir cihaz örneği, temel ya da diğer kodlar ile beraber üretilen bu temel ya da diğer kodların zamanını tanımlayan bir zaman kodunu da iletir. Zaman kodunun iletilmesi her zaman şart değildir. Bazı durumlarda iletilmeyebilir. Pozisyon ve zaman bilgileri harici bir iletişim sisteminden de belirlenebilir.

[24]'de E.Ayeh sıfır bilgi ispatını (Zero Knowledge Proof) temel alan kimlik doğrulama protokolü önerir. Bu protokol kimliğimiz ile ilgili hiçbir bilgi ortaya çıkarmadan kimliğimizi kanıtlamanın güzel bir yöntemidir. Kuzey Teksas Universitesi (UNT) Sıfır Bilgi İspatı protokolünü tasarlamak, geliştirmek ve havacılık ağlarına uygunluğunu belirleyebilmek adına Hava Kuvvetleri Araştırma Laboratuarı ile beraber çalışmıştır. Bu aşamada Graph Isomorphism (GI) tabanlı Sıfır Bilgi ispati protokolünü seçmişlerdir. ZKP protokolünü graf izomorfizm şemaları kullanarak başarılı bir şekilde uygulamışlardır. Uygulama için uygun graf seçimi yapmaları gerekliydi. Düşük otomorflu (bir otomorfa sahip) düzenli grafları ya da daha yüksek graf izomorfizm karmaşıklığına sahip grafları kullanmış olsalar bile, bu düzenli grafların Nauty [25] gibi araçlar kullanılarak hala kırılabildiklerini görmüşlerdir.

IFF Mode 5, ağ ile bağlanmış savaş alanları için unique ID, zaman ve coğrafi pozisyonlar gibi veriler sağlar. Mode 5 otomatik geçişli black key kullanılan yeni bir şifreleme algoritmasına sahiptir. PIN (Platform Kimlik Numarası) ve National Origin

(NO) kombinasyonları transponder için unique bir Mode 5 tanımlayıcısı sağlayacaktır. Amerika ve NATO orduları şu anda NATO Standart Anlaşması 4193 (STANAG 4193)'de tanımlanmış olan ve kriptografik olarak korunan Mode 4 ve Mode 5 dahil olmak üzere farklı standartlar kullanmaktadırlar [26].

Baek ve arkadaşları Kimlik tabanlı şifreleme (IBE) şeması önerir [27]. E-enable uçağı güvence altına almanın temel işlevsel sorunlarından biri, PKI'nın açık anahtar şifrelemesine dayalı gizlilik ve kimlik doğrulama hizmetleri sağlamak için kullanılacak ölçeklenebilirliğidir. Kimlik Tabanlı İmza'nın (IBS) bu sorun için umut verici bir çözüm olabileceğini savunuyorlar. E-enabled hava araçları, bir kez Identity-Based Signature(IBS) ile donatıldığında; önceden yüklenmiş sertifikalara veya sertifikalarla birlikte verilmesi gereken kendi açık anahtarlarına (public key) ihtiyaç duymazlar. Bu metotta, ICAO tarafından belirlenmiş olan kısa süreli uçuş bilgileri de dahil olmak üzere benzersiz göstergeler uçağa tanımlanmıştır. Uçak merkezdeki havalimanlarından birinden havalandığında, havayolu dağıtım noktasında kimliği ile ilişkilendirilen gizli anahtar ile yüklenecektir. Uçak bu gizli anahtarı uçuş süresince kendisinden çıkan ADS-B Out gibi giden verileri imzalamak için kullanacaktır. Böylece bu gizli anahtar hem havadan havaya, hem de havadan yer istasyonuna kurulan iletişimde kimlik doğrulamasını sağlayacaktır. [20] 'deki çalışma havadan havaya iletişimde ADS-B In teknolojisinde bir şifreleme şeması sunmuştur ve IBE şemasının avantaj ve dezavantajlarını göstermiştir. Uçakların her havalanma öncesinde gizli anahtarları ile yüklenmeleri gerekmesi, uçuş öncesinde ekstra bir operasyonel yük getirecektir. Ayrıca ICAO tarafından kalkışı yönetilmeyen uçuşlarda (IOT cihazları, dronelar gibi) bu anahtarların yüklenememesi ve bu cihazlardan gelen verileri doğrulayamayacak olmamız metodun dezavantajlarından biridir.

E. A. El-Badawy ve arkadaşları, dost düşman tanıma sistemleri için bu makalede [28] yeni bir yöntem öneriyor. Bu yöntemin temelinde Mode-S IFF ile Chaos Advanced Encryption Standard (AES) kullanılması yatıyor. Kimlik doğrulama sürecindeki her dost uçak sorgulamaya sorguyu yapan radar istasyonunun bulunduğu bölgenin gizli kodlarıyla cevap verir. Radar istasyonu da kodların geçerliliğini kontrol eder. Bu makale Mode-S IFF eski sistemi ile uyumlu yeni bir sivil havacılık uygulamalarıyla da kullanılabilen dost düşman tanıma sistemi önerir. Gelişmiş Şifreleme Standardı (AES) bu algoritmada kullanılır. AES hesaplama açısından yoğun ve paralel bir yapıya

sahiptir. Bu da uygulayıcılara etkili kripto saldırılara karşı çok fazla esneklik sağlar. Algoritmanın işlemlerinde 128 bitlik bir şifre anahtarı ve 128 bitlik mesaj blokları kullanılır. İlk koşullara duyarlı, yörüngelerden tüm aralık boyunca yayılan ve daha fazla güvenlik ve gizlilik için ikinci bir anahtar olarak kullanan yeni bir kaotik S – kutusu dağıtımı uygular. Elde edilen sonuçlarda, rastgele S - kutusu ve kaotik S - kutusu arasındaki farklı başlangıç koşullarındaki frekans, çalışma ve seri testleri için performans karşılaştırması bulunmaktadır.

Bugün IFF sistemleri kriptografik tanıma şemalarına dayanan sorgu–yanıt (Challenge – Response) temelli bir protokol kullanmaktadırlar [29]. Kodlar çeşitli modlarda dost birimler arasında kararlaştırılmış ve dağıtılmıştır. Gelen bir istek yalnızca bu kodlarla yanıt verirse arkadaş olarak tanımlanır. Kimlik doğrulama şemasının güvenliğini göstermek için, sıfır bilgi kavramından ziyade tanık-gizleme kavramını(witness-hiding) [30] kullanırlar. Bu çalışmalarında mafya sahteciliğine(mafia frauds) direnen bir tanımlama şeması tasarlamışlardır, tanımlama sistemlerinin birçok pratik güvenlik problemini çözebildiklerini iddia etmişlerdir. Çoğunlukla, eş zamanlı ortamda mafya sahtekârlığı atağına karşı sıfır bilgi ispatının güvenli olduğu kanıtlanmamıştır.

Ortak asimetrik şifreleme yöntemlerini temel alan ve IFF sistemlerinin güvenliğini daha da öteye taşıtan özel bir kimlik doğrulama şeması sunmuşlardır [31]. Kanal Atlama(Channel Hopping) sistemin sıfır bilgi ispatı olup olmadığını kanıtlamak şu anda ucu açık bir sorudur. Mevcut tanıma şemalarının fiziksel objeleri güvenli şekilde tanıma sorununu çözemediğini iddia etmişlerdir. Kanal atlama (channel hopping) teknolojisine dayanan yeni bir yaklaşım önerirler. Yaklaşımlarının temel unsuru, gizlice dinlenmeyi engellemek için rastgele kanallardan oluşan bir kanal atlama sisteminin kullanılmasıdır. Diğer çözümlerin aksine, doğrulayan(verifier) ve ispatlayan(prover) arasında yarı güvenli-yeni bir anahtar paylaşıldığını öneriyorlar.

N. İkram ve arkadaşları [32] kapalı ağlara katılmaya çalışan kullanıcılara yeni bir kimlik doğrulama şeması önerir. Burada önerilen yeni teknik, açık anahtarlı kriptografi kavramına dayanmaktadır. Güvenlik, kendisinin bir ikili sonlu alan üzerinde tanımlandığı eliptik bir eğri boyunca (EC) ayrık logaritmaların kullanılmasına dayanır. Bu yeni metodu uygulamak için Galois Alanları (Galois Fields) üzerinde tanımlanan eliptik eğrileri kullanırlar. Kimlik tabanlı şifreleme yöntemi bu çalışmanın

da temelde kullandığı tekniktir. Bu yüksek doğruluktaki IFF protokolü kullanıldığında, tüm mesajlar bir düşman tarafından ele geçirilebilse bile tanıma(Identification) bütünlüğüne zarar getirmediğini iddia etmişlerdir. Bu çalışmada sunulan şifreleme yaklaşımı sayesinde, tanıma işlemi, gizli mesajların şifrelenmiş biçimde değişimi olmaksızın gerçekleştirilebilir. Aynı ID tabanlı şifreleme sistemi konseptini kullanarak, önerilen sistemin ATM'lerde ve benzer nitelikteki diğer uygulamalarda da uygulanabileceğini söylemektedirler.

Önerdiğimiz yöntem, grafik izomorfizmi kullanan diğer ZKP yöntemleri kadar karmaşık değildir. Dahası, sadece askeri uçaklar için kullanılabilir değildir. Kullandığımız tanımlama şeması, havacılık dışındaki diğer sistemler tarafından da kullanılabilir, örneğin IoT cihazlarda. Uygulama maliyeti daha düşüktür diğer yöntemlere göre, çünkü zamana bağlı değişen IFF kodları kullanmıyoruz. Operasyonel maliyeti bu yüzden daha düşüktür. Gizlice dinleme saldırıları için daha güvenilirdir. Sıfır bilgi ispat algoritmasını kullandığımız için, saldırgan herhangi bir gizli bilgiyi yakalayamaz, manipüle edemez. Bölüm 4'de yöntemimiz detaylı bir şekilde anlatılmıştır.

3.1 Sorgu –Yanıt (Challenge – Response)

Literatürde kullanılan yöntemlerden biri de "Challenger–response teknik" olarak adlandırılan sorgulama –yanıtlama kimlik doğrulama tekniğidir. Sorgulama-yanıt protokolleri, güvensiz kanallar üzerinden kimlik doğrulama için yaygın olarak kullanılmaktadır. Bu teknik, ordunun dost ve düşman uçaklarını tanımlamak için kullandığı IFF'e benzer. Örneğin kullanıldığı diğer bir alan paralo güvenliği sorunudur, parolalarla ilgili temel bir sorun, parolaların tekrar tekrar kullanılmasıdır. Bu parolalar ele geçirildiğinde, kimlik doğrulama sistemi gerçek kullanıcının şifreyi girip girmediğini veya sahtekârın şifreyi elde edip etmediğini belirleyemez. Bu duruma karşı koymak için geliştirilen strateji, bir şifrenin sadece bir kez kullanılmasına izin vermektir. Birkaç farklı sorgu-yanıt sistemi vardır. Challenge-Response Authentication'da kullanılan şifreleme protokolü, kullanıcının şifresini açıklamadan şifreyi bildiğini ispat etmesine izin verir.

Tanım: K kullanıcısı, kendini S sistemine doğrulamak istiyor. K ve S üzerinde anlaşmaya vardığı gizli bir f fonksiyonu var. Bu sorgu-yanıt kimlik doğrulama sistemi,

S'nin K'ya rastgele bir m mesajı gönderdiği bir sorgu sistemidir. K yanıt olarak r = f(m) dönüşümü yaparak cevap verir. S, r'yi ayrı ayrı hesaplayarak doğrular.

3.2 Kimlik Tabanlı İmza (Identity Based Signature – IBS)

Kimlik tabanlı imza yöntemi 1984'te Shamir tarafından tanıtılmıştır [33]. Geleneksel imzalama şemalarında yer alan anahtar özgünlüğüne bağlı kimlik doğrulama yapar bu yöntem. Bu şifreleme tekniği, herhangi bir kullanıcının, gizli(private) veya açık(public) anahtarlarını değiş tokuş etmeden, anahtar dizinleri tutmadan ve üçüncü taraf hizmetleri kullanmadan güvenli bir şekilde iletişim kurmasını ve birbirlerinin imzalarını doğrulamalarını sağlayan bir şifreleme türüdür. Bu imza şemalarında kişiye özgü (isim, e-posta adresi vb.) kimlik bilgileri imza ile ilişkilendirilir. IBS, PKI sertifikalarının geçerliliğinin kontrol edilmesi gerekliliğini ortadan kaldırmaktır.

Kimlik Tabanlı İmza (IBS) şemasında, imzalayan, tanımlayıcı kimlik bilgisini gizli anahtar üretecine (PKG) kaydeder. Daha sonra PKG, tanımlayıcı kimlik bilgisini kullanarak kimliğiyle ilişkilendirilmiş gizli anahtar sk_{ID}'sini hesaplar. Bob'un tanımlayıcı kimlik bilgisi e-posta adresi, telefon numarası ve benzeri herhangi bir bilgiden kolayca hesaplanabilir. İmzalayan kişi, PKG'den sk_{ID} edindikten sonra karşılık gelen imzalar oluşturmak için bir mesaj imzalayabilir. Bu mesajı kullanarak imzalayanın kimlik bilgisi ve imza ile, Alice imzanın geçerli olup olmadığını kontrol edebilir. IBS'nin dijital sertifikaların kullanımından kaçınır, ancak her kullanıcı örtük sertifikalandırılır. Bu kullanıcılar tanımlayıcısını başarıyla kaydeden ve karşılık gelen gizli anahtarı alan kullanıcıdır. Şifrelemede, örtük sertifikalar, açık(public) anahtar sertifikasının bir çeşididir, açık anahtar yeniden yapılandırılabilir ve herhangi bir örtük sertifikadan dolaylı olarak doğrulanabilir; örtük sertifikada tanımlanan tarafın, ilgili gizli(private) anahtarı bilen tek kişi olduğu anlamına gelir. Bu, gizli anahtarın kimsenin bilinmediği olasılığını yok saymaz, ancak bu olasılık önemli bir sorun olarak kabul edilmez.

Bir IBS şeması, her biri aşağıda tarif edilen, aşağıdaki polinom-zaman algoritmalarından oluşur, Şekil 3.1 'de gösterilmiştir:

1. Kurulum(Setup)

   Girdi olarak güvenlik parametreleri alınır, bu algoritma gizli ana anahtarı

(msk) ve Gizli Anahtar Üreticisi (PKG)'nin genel parametrelerini $(params)$ oluşturur.($params$ şemadaki tüm alt algoritmalara girdi(input) olarak sağlanır).

2. Gizli Anahtar Üretme (Extract)

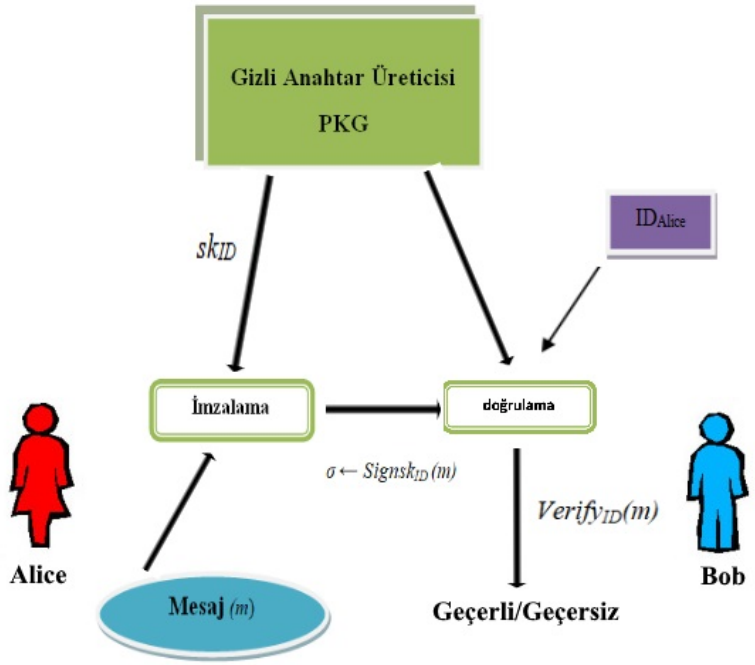
   ID kullanıcının kimliğidir. Bu algoritma ID ve msk'yı alarak, kullanıcıya güvenli bir şekilde gönderilecek olan , kimlik bilgileriyle ilişkilendirilmiş sk_{ID} gizli anahtarını oluşturur.

3. İmzalama(Sign)

   Algoritma, ID ve mesaj m ile ilişkilendirilmiş imzalama anahtarını sk_{ID} girdi olarak alarak, m'nin σ imzasını oluşturur $\sigma \leftarrow Signsk_{ID}(m)$.

4. Doğrulama(Verify)

   Girdi olarak ID, mesaj m ve imza σ alan bu algoritma, σ'nun m'nin gerçerli bir imzası olup olmadığını kontrol eder. Eğer σ geçerliyse algoritma çıktısı $gecerli$ değilse $gecersiz$'dir. $valid/invalid \leftarrow Verify_{ID}(m)$.



Şekil 3.1 : Kimlik tabanlı imza şeması.

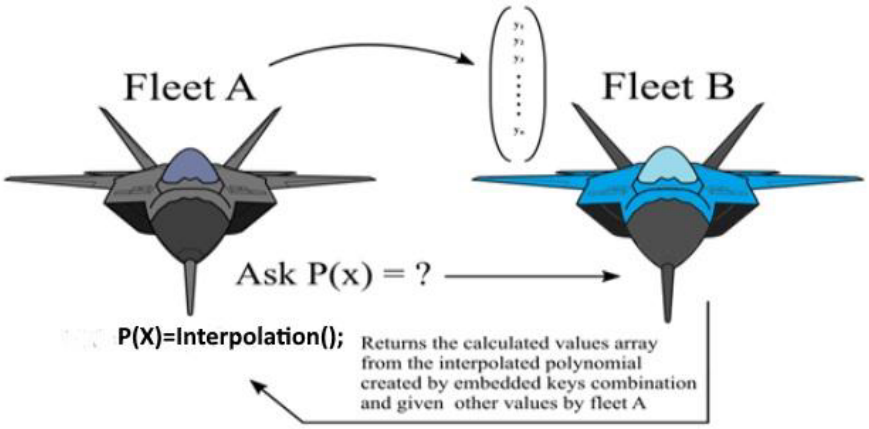
4. ÖNERİLEN YÖNTEM

Güvenli tanıma yöntemi, klasik kriptografik yöntemlerin ve sıfır bilgi ispatı yöntemlerinin bir birleşimidir. Aynı filoya ait uçaklar aynı anahtar değer ile yüklenirler ve diğer dost filo uçakları ile daha önceden belirlenilmiş bir oranda anahtarlarları benzerlik içerir. Bu çalışmada yarattığımız matematiksel modelde dost uçaklardaki anahtarların birbirlerine açıklanmadan benzer olduğunu tespit etme çalışması hazırladık, sorgulayıcı tarafından teyit edilen bilgiye göre karşı taraftaki uçak dost/bilinmeyen kategorisine sokuluyor. Modelde, uçağın anahtarını paylaşmadan diğer uçaktaki anahtarla benzer noktalarının doğruluğunu kanıtlamak için Zero Knowledge Proof tekniklerinin bir çeşidini kullanıyoruz. Polinom interpolasyonuna dayalı doğrulama süreci gerçekleştiriyoruz. Polinom interpolasyonu ve sıfır bilgi ispatı hakkında kısa bir özet sonraki alt bölümde sunulmuştur (Şekil 4.1).

Kullanılan yöntemde her iki taraf (sorgulayan ve cevaplayan) da temel olarak polinom interpolasyonu yapar ve sorgulayan belirli bir noktadaki değer kümesi sonuçlarının cevaplayan tarafla aynı olması durumunda iletişime geçilen kişiyi "dost" olarak işaretlerken, aynı olmaması durumunda da "bilinmeyen" olarak işaretler.

Sorgulayan tarafta n adet gömülü anahtar mevcuttur. Bu gömülü anahtarlardan daha önce ortak olduğunu bildiği kararlaştırılmış c adet anahtarı interpolasyon yapılacak polinomun X_i değerleri olarak kararlaştırılır. Sorgulayıcı taraf Y_a tane rastgele değer üretir. Y_a ' lar arasından daha önce ortak olduğunu bildiği gömülü anahtarların indeks seviyesine denk gelen değerleri ise Y_i polinomda kullanılmak üzere kararlaştırılır. Daha sonra X_i ve Y_i değerleri kullanılarak bir polinom oluşturulur ve rastgele üretilen Z noktasındaki polinomun değeri D hesaplanır. Bütün bu işlemler mod M' de yapılır. Bu aşamada rastgele üretilmiş olan Y_a değerleri ve Z değeri cevaplayıcı tarafa gönderilir ve gelecek cevap beklenir. Cevap geldikten sonra gelen değerler arasında D değeri' nin olup olmadığına bakılır. D değeri gelen değerler arasında varsa cevaplayıcı dost, yoksa bilinmeyen olarak işaretlenir.

Cevaplayıcı tarafta ise yine n adet gömülü anahtar mevcuttur. Bu n adet gömülü anahtarın C sayısındaki kombinasyonları K adet olmak üzere hesaplanır. K adet hesaplanan her kombinasyonlardaki değerler X_i olarak seçilir ve bu indekslere karşılık gelen sorgulayıcı taraftan alınan Ya değerleri arasından Y_i değerleri seçilir. Bu değerler ile K adet polinom enterpolasyonu yapılır ve yine sorgulayıcı taraftan alınmış olan Z noktasındaki polinomların değeri hesaplanır. Bu şekilde K tane P(Z) değeri bulunur. Buradaki bütün işlemler de yine daha önce kararlaştırılmış olan mod M' de yapılır. Daha sonra K adet hesaplanmış polinom değeri sorgulayıcı taraf ile paylaşılır.



Şekil 4.1 : Güvenli tanıma yöntemimizin filolar arası haberleşme şeması.

4.1 Matematiksel Arka Plan

Sonlu cisimler ile çalışmak pek çok durumda daha uygun olacaktır. Örneğin $\frac{1}{3}$ mod 43'de 29 mod 43 olarak yazılıyor. Yani $\frac{1}{3}$ yerine 29 ile calismak daha kolaydir. Genel kural, eğer $\gcd(y,n) = 1$ ise $\frac{x}{y}$ kesiri mod n olarak kullanılabilir. Aslında, $\frac{x}{y}$ mod n, $y^{-1}x$ mod n anlamına gelir; burada y^{-1}, $y^{-1}y \equiv 1$ mod n'i sağlayan tamsayıyı belirtir. Ama örneğin; $\frac{1}{4}$ mod 4 kullanamayız, çünkü bu 0 mod 4 'e bölmek anlamına gelir. Sadece $\frac{1}{2}$ mod 4 ile çalışsak bile işler daha karmaşık hale gelir. Örneğin, $2 \equiv 6$

$\bmod 4$, ancak $1 \not\equiv 3 \mod 4$ olduğundan her iki tarafı da $\frac{1}{2}$ ile çarpamayız. Problem şu ki $\gcd(2,4) = 2 \neq 1$ 'dir. 2, 4'ün faktörü olduğundan 2'ye bölmeyi kısmen 0'a bölmek olarak düşünebiliriz. Hiçbir durumda buna izin verilmemektedir. Aslında bizim sayıların tersine (y^{-1}) ihtiyacımız var. Şimdi bu amaçla hareket ederek ilk olarak, iki tamsayının en büyük ortak bölenini bulma yöntemini ele alacağız. Daha sonra, gcd kullanarak y^{-1} elde edeceğiz.

4.1.1 En büyük ortak bölenin bulunması: Öklid algoritması

Farz edelim ki $b < a$, eğer değilse a ve b yer değiştirilir. İlk adımda a, b 'ye bölünür ve a aşağıdaki formda yazılır:

$$a = q_1 b + r_1.$$

Eğer $r_1 = 0$ ise b, a'yı böler ve en büyük ortak bölen b'dir. $r_1 \neq 0$, ise; b'yi aşağıdaki formda yazarak devam edin:

$$b = q_2 r_1 + r_2.$$

Kalan sıfır oluncaya kadar aşağıdaki şekilde devam edin :

$$a = q_1 b + r_1$$

$$b = q_2 r_1 + r_2.$$

$$r_1 = q_3 r_2 + r_3.$$

$$r_{k-1} = q_k r_{k-1} + r_k.$$

$$r_{k-1} = q_{k+1} r_k + 0.$$

Sonuç :

$$\gcd(a,b) = r_k.$$

Bu algoritmanın iki önemli yönü vardır :

- Sayıların çarpanlara ayrılması gerekmez.
- Hızlıdır.

Teorem 1 a ve b, en az biri sıfırdan farklı olmak üzere iki tamsayıdır ve $d = \gcd(a,b)$'dir. $ax + bx = d$ eşitliğini veren x, y tamsayıları her zaman vardır. Özellikle eğer a ve b aralarında asal ise $ax + by = 1$ eşitliğini sağlayan x ve y tamsayıları vardır.

4.1.2 Tersini bulma

a, $\gcd(a,n) = 1$ olacak şekilde bir tam sayı olsun. Öklid algoritması kullanılarak $ax + ny = 1$ olarak yazılabilir. Bu denklem $\mod n$'e göre düşünüldüğünde $ax \equiv 1$, yani x, a'nın tersi, $\frac{1}{a} = x$ elde edilir.

Örnek $\frac{12}{5} \mod 7$'yi hesaplayalım. Bu ifade aynı zamanda şudur: $\frac{12}{5} = 12.5^{-1} \mod 7$. $\mod 7$'ye göre hesaplanmış 5'in tersine ihtiyacımız var. Öncelikle Öklid algoritmasını kullanarak en büyük ortak böleni hesaplayalım :

$$7 = 1.5 + 2$$

$$5 = 2.2 + 1$$

$$2 = 2.1 + 0.$$

$\gcd(5,7) = 1$ ve $3.5 - 2.7 = 1$'dir. Denklemi $\mod 7$'de göz önüne alırsak $3.5 \equiv 1 \mod 7$'dir. Bu da şu anlama gelir: $5^{-1} \equiv 3 \mod 7$. Dolayısıyla $\frac{12}{5} = 12.5^{-1} = 12.3 \equiv 1 \mod 7$.

4.1.3 Polinom interpolasyonu

Temel bir matematiksel teknik karmaşık bir şeyi basit ya da en azından daha az karmaşık olana yaklaştırmaktır, ama bunu yaparken de orijinal bazı temel bilgileri içermesi beklenir. Farklı x koordinatlarına sahip n adet (x_i, y_i) nokta vardır. Bu noktaların her birinden geçen maksimum $n-1$ dereceli polinomu bulmak için polinom interpolasyonu bir yöntemdir.

İnterpolasyon yapan polinomlar, verilerin etkin şekilde genişletilmesini sağlayan veri noktası yaklaşımı sağlar. Bu yöntemler genellikle karmaşık fonksiyon değerlerini hesaplamak ve diferansiyel denklemleri değerlendirebilmek için sayısal yaklaşımlar sunarlar. Polinom interpolasyonu yöntemleri yüzlerce yıl öncesine dayanmaktadır. Herhangi bir polinom interpolasyonu problemi, katsayıları lineer bir sisteme çözüm olarak uygulayarak çözülebilir. İnterpolasyon, ölçülen noktalar tarafından gerilen bir bölgede analitik ifadeyi, özel olarak bir fonksiyonu, tahmin etmek için basit ve iyi bir yol sağlar.

4.1.4 Newton bölünmüş farklar metodu

Bölünmüş farklar yöntemi, bir dizi noktası verilen polinomu interpolate etmek için kullanılan sayısal bir prosedürdür. Temel fikir interpolasyon noktalarını içeren doğrusal faktörleri kullanan Newton formunu kullanarak interpolasyon yapan polinomları temsil etmektir. $n+1$ adet noktamızın olduğunu varsayalım. Bunlar $(x_0,y_0),(x_1,y_1),...,(x_{n-1},y_{n-1}),(x_n,y_n)$. Bölünmüş fark polinomunun genel formu şu şekilde yazılır

$$f_n(x) = b_0 + b_1(x-x_0) + b_2(x-x_0)(x-x_1) + ... + b_n(x-x_0)(x-x_1)...(x-x_{n-1})$$

$$b_0 = f[x_0]$$

$$b_1 = f[x_1,x_0]$$

$$b_2 = f[x_2,x_1,x_0]$$

$$\vdots$$

$$b_{n-1} = f[x_{n-1},x_{n-2},...,x_0]$$

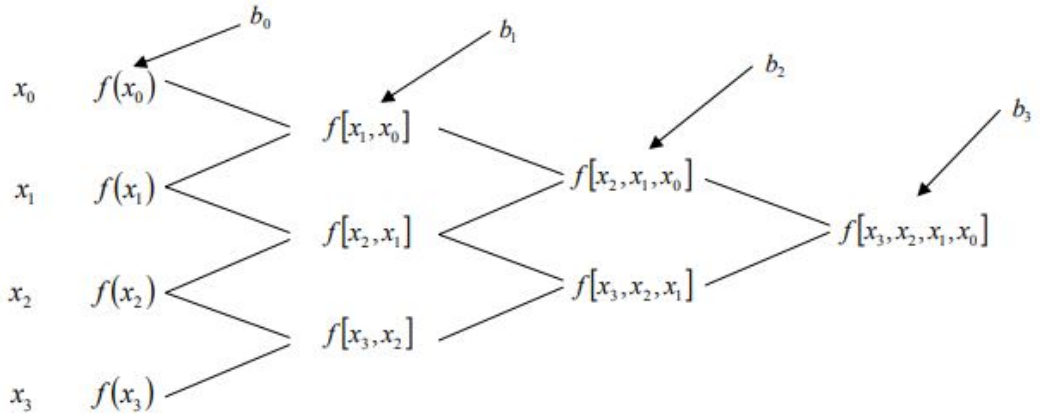
$$b_n = f[x_n,x_{n-1},...,x_0]$$

m^{th} bölünmüş farkın tanımı

$$b_m = f[x_m,x_{m-1},...,x_0] = \frac{f[x_m,x_{m-1},...,x_1] - f[x_{m-1},x_{m-2},...,x_0]}{x_m - x_0}. \tag{4.1}$$

Bölünmüş farkların tekrarlı bir şekilde hesaplandığı kolayca görülebilir (Denklem 4.1). Ayrıca, interpolasyon *modulo* p üzerinde düşünülebilir, katsayı b_i, p dereceli alan içindeyse. $\frac{f[x_m,x_{m-1},...,x_1]-f[x_{m-1},x_{m-2},...,x_0]}{x_m-x_0}$ yerine $(f[x_m,x_{m-1},...,x_1] - f[x_{m-1},x_{m-2},...,x_0])(x_m-x_0)^{-1}$ hesaplanır. Burada $(x_m-x_0)^{-1}$ F_p'deki (x_m-x_0)'nin tersidir (Şekil 4.2).

Newton polinom interpolasyonunun kullanıldığı bazı çalışmalar:
Bu makalede [34] Lin CH ve arkadaşları Newton polinom interpolasyonu yapan ve DES (veri şifreleme standardı) gibi güçlü bir şifreleme işlemine dayanan bir şifre doğrulama mekanizması önermişlerdir. Newton polinom interpolasyonu kullanarak yüksek sistem performansı elde etmişlerdir.



Şekil 4.2 : Bölünmüş fark gösterimi.

Bir diğer çalışmada da Chang ve arkadaşları [35] kullanıcı hiyerarşisinde erişim kontrolü için bir şifreleme anahtarı atama şeması önerilmiştir. Önerdikleri yöntem Newton interpolasyon yöntemine ve önceden tanımlanmış tek yönlü fonksiyona dayanır.

Geleneksel bilgisayar sistemlerinde, kritik verilerin korunması için kullanıcı doğrulama, genellikle şifre doğrulama ve erişim kontrolü ile sağlanır. Bu makalede [36] bilgisayar koruma sisteminin erişim matrisini uygulamak için kullanılan yeni tek tuşla kilitleme(single-key-lock SKL) mekanizması önerilmiştir. Anahtar seçimi çok esnektir. Kilit değerleri, Newton polinom interpolasyonuna dayanarak tekrarlı bir şekilde üretilir. Sisteme yeni bir kullanıcı / dosya eklenmesi, tüm kilitlerin yeniden hesaplamadan başarıyla uygulanabildiğini göstermişlerdir. Burdaki temel koruma mekanizması Newton'un polinom interpolasyonudur.

4.1.5 Sıfır bilgi ispatı (Zero Knowledge Proof) ve sır paylaşımı(Secret Sharing)

Kriptografide güvenli iletişimi sağlayan birçok farklı algoritma vardır. Bu çalışmada, özel olarak Sır Paylaşımı ve Sıfır Bilgi İspatı(ZKP) olmak üzere iki algoritma kullanacağız.

Sıfır bilgili ispatı (ZKP) sistemleri, 1985 yılında Goldwasser, Micali ve Rackoff [37] tarafından tanıtıldı. Bu protokol bir Prover'ın (ispatlayıcı) bir Verifier'ı (doğrulayıcı) bilginin gerçekliliğinin ötesinde hiçbir bilgi açığa çıkarmadan bilginin geçerliliğine ikna etmesine dayanır. Bilinen gerçek, yalnızca talebin doğru olduğu ve başka

hiçbir bilginin açıklanmadığıdır. Verimli olarak hesaplanamadığı bilinen farklı problemlerin (Graph Isomorphism ve Graph Non-Isomorphism gibi) sıfır bilgi ispatı sistemlerini kabul ettiği gösterilmiştir [37, 38]. Sıfır bilgi teknikleri, kriptografik algoritmalarda kullanılan en önemli araçlardan biridir. Eşsiz yapıları nedeniyle çok çeşitli uygulamalara sahiptirler. Kurulduğundan beri, ZKP sistemleri modern şifreleme ve özellikle de kimlik doğrulama gerektiren güvenlik protokollerinde yapı taşları olarak uygulamalara sahiptir. Kimlik doğrulama prosedürü sırasında Prover, Verifier tarafından bir dizi tanıma turu sırasında ortaya konan sorulara cevap vermelidir. Kimliğini kanıtlamak için, Prover tüm sorulara başarıyla cevap verebilmelidir. Verifier'ın, Prover'ın kimliğine olan güveni her turda artar. Verifier, ZKP protokollerinde doğrulama prosedüründen hiçbir şey öğrenemez. Ek olarak, Verifier Prover'ı kandıramaz, çünkü Prover'ın gizli bilgisini hesaplayamaz. Ayrıca, Verifier Prover'ı kandıramaz çünkü protokol Verifier ikna olmadıkça tekrar edilir. Rastgele bir soru seçildiği için Verifier üçüncü bir tarafa Prover gibi davranamaz. Bu nedenle, Prover'ın kimliğini kanıtlaması için gerekli olan ek hesaplama yükü, RSA gibi güvenilir bir üçüncü tarafa ihtiyaç duyan diğer kimlik doğrulama yöntemlerinden önemli ölçüde daha düşüktür. ZKP sistemlerinin kaynak sınırlı sistemlere çok uygun olduğu düşünülmesinin ana nedeni budur [39].

Tamsayı olarak temsil edilen bir M mesajınızın olduğu farz edelim. Bu mesajı Alice ve Bob arasında ikisinin de ayrı ayrı mesajı yeniden oluşturamayacağı bir şekilde bölüştürmek istiyoruz. Bu sorun kolayca şöyle çözülebilir: Alice'e rastgele bir r tamsayısını ve Bob'a $M - r$'yi vererek M mesajını yeniden oluşturmak için Alice ve Bob parçaların birleştirmek zorundadırlar. Bu prosedür sır paylaşım şeması olarak bilinir.

Tanım : $t \leq w$ ve t, w pozitif tamsayılardır.(t, w) şeması M mesajını bir grup w arasında paylaşır, t kadar katılımcıdan oluşan herhangi bir alt küme M mesajını yeniden oluşturabilir, ancak daha küçük boyutlu alt kümeler M'yi yeniden oluşturamaz.

Öte yandan, birçok durumda bir işlemi tamamlamak için birisi bir şifre veya kimlik numarasını kullanmak zorunda kalabilir. Eğer kötü niyetli bir kişi bu sırrı elde ederse, kendini orijinal kişinin yerine koyabilir ve onun gibi davranabilir.

Bu gereksinime dayanan çeşitli matematiksel prosedürler vardır ve bunlara sıfır bilgi teknikleri denir. Nitekim asıl amaç, gizli dinleyicinin tekrar kullanabileceği herhangi bir bilgi vermeden sırrı kullanmaktır.

4.2 Uygulama

Diğer sistemlerde olduğu gibi, uçakların da birbiriyle iletişim kurarken güvenliğe ihtiyacı vardır. G_1 ve G_2 iki uçak filosu olsun. G_1 ve G_2 iletişim kurmak istiyor ve G_1 bir G_2 üyesinin dostça olup olmadığını belirlemek istiyor. G_1 ve G_2'nin ayrı ayrı 1024 bitlik bir x_n ve ${x^*}_n$'ye karşılık gelen n adet veriye sahip olduğunu varsayalım. Bir uçak dostsa k adet x_i verisi aynıdır. Her x_i için rastgele y_i üretilir ve y_i'ler açık kanalda yayınlanır. G_1 tarafından k tane (x_i, y_i) noktaları kullanılarak k-1 dereceli $p(x)$ polinomu yaratılır. Diğer filodaki uçaktan $p(x)$'in seçilen bir noktasındaki değerini, $p(a)$, ister. Değer eşleşirse, bunun dost bir uçak olduğuna karar verir. G_2'nin diğer filo ile k kadar (x_i, y_i) noktası sıra bilinmeksizin aynıdır. $\binom{n}{k}$ adet polinom yaratılır ve her bir polinom verilen değer için hesaplanır. G_1 , kendi hesapladığı değerle gönderilen değerin eşleşip eşleşmediğini kontrol eder. Daha sonra, G_2'nin dost bir uçak olduğuna karar verir.

Tüm olası mesajlardan ve n sayısından daha büyük olması gereken bir asal p sayısı seçilsin. Tüm hesaplamalar $\bmod p$'de gerçekleştirilecektir. Eğer asal olmayan bir sayı kullanılırsa, güvenlik açıkları olabilir.

4.2.1 Algoritma

G_1 filosundan herhangi bir uçağın 10 adet $x_1, x_2, ...x_{10}$ 1024 bit'lik verisi vardır. x_i'ye karşılık gelen rastgele y_i üretilir. Daha sonra,G_1, 10 tane noktadan herhangi 6 noktasını kullanarak x_1, x_2, x_3, x_4, x_5 denklem 4.2'deki 5 dereceli polinomu interpolate eder :

$$p(x) = b_0 + b_1(x - x_1) + b_2(x - x_1)(x - x_2) + ... + b_5(x - x_1)(x - x_2)...(x - x_6). \quad (4.2)$$

Polinomu interpole ederken, diğer algoritmalardan daha hızlı olan Newton'un bölünmüş farklar metodu kullanılabilir. Rastgele bir a seçilir ve $p(a)$ hesaplanır. Eğer G_2 grubundan bir uçağın G_1 filosundan bir uçak ile ortak 6 değere sahipse bunların sıralarını bilmediği için bu noktaları kullanarak $\binom{10}{6} = 210$ adet polinom interpole

eder ve interpole edilen polinomların her biri için a değerini koyarak hesaplama yapar ve G_1 filosundaki uçağa gönderir. G_1 filosundaki uçak kendindeki değerle G_2 filosundaki uçağın gönderdiği değerleri karşılaştırır. İçinde kendi yarattığı değer varsa G_2filosundaki uçağı dost olarak belirler. Eğer herhangi bir uçak G_1 filosundaki uçak ile eşleşen 6 noktaya sahip değilse, 5 veya daha az aynı noktaya sahipse bile, $p(a)$'dan aynı sonucu elde edemez. G_1 filosundaki uçak da onu bilinmeyen olarak işaretler. Metodun adımları algoritmik olarak şöyle açıklanabilir :

1. x_i'ler ile eşleşen rastgele y_i değerleri oluşturulur. 10 adet farklı (x_i, y_i) noktası olacaktır.
2. Bunlardan 6 nokta kullanılarak 5. dereceden $p(x)$ polinomu interpolate edilir.
3. a sayısı seçilerek $p(a)$ hesaplanır.
4. Diğer grup kendi 10 verisinden 6 nokta seçerek $\binom{10}{6} = 210$ farklı ${p_i}^*(x)$ polinomu yaratır.
5. Bu 210 farklı polinom için ${p_i}^*(a)$ hesaplanır.
6. Eşleşme kontrol edilir. Eğer bazı $i = 1,2,...210$ için $p(a) = {p_i}^*(a)$ ise eşleşme vardır ve ilk grup diğer grubu dost olarak işaretler. Aksi takdirde uçak bilinmeyen olarak işaretlenir.

Rastgele belirlenen ve yayınlanan y_i'ler ve a açık kanaldan gönderilir. Ama x_i'ler gizlidir.

İşlem ayrıca, yeterince büyük olan bir asal sayıya göre çalışır. Güvenlik seviyesi konusunda mod p'deki modüler aritmetik avantaj sağlar. İlk veriler süreç ilerledikçe farklı görüneceğinden, saldırganların bilgi yakalama şansı azaltılacaktır. Ayrıca, modüler aritmetiğin kullanılmasının temel sebeplerden biri, çoğu modern açık anahtar şifreleme sisteminin temel yapı taşları olan grupları, halkaları ve cisimleri kolayca oluşturmamıza izin vermesidir. Bu nedenle, özellikle uçaklarda olmak üzere birçok yerde güvenli iletişim için avantaj sağlar.Burada hem sıfır bilgili ispatı hem de sır paylaşım şemasını kullanıyoruz.

Diğer taraftan, x_i'ler ve sıraları hakkında herhangi bir bilgi bilinmeyecektir. Ayrıca, herhangi bir tarafın 6'dan daha az eşleşmiş verisi varsa, o zaman dost uçak gibi davranamayacaktır.

4.2.2 Pseudo kod

Algorithm 1 Alice' in Fonksiyonu

1: **function** BOBARKADASMI(K_a, M_a, n, m) ▷ K_a : gömülü anahtar değerleri dizisi, M_a : diğer birimler ile ortak gömülü anahtarların bit değerleri, n : anahtarın uzunluğu, m : mod değeri olmak üzere
2: i=1
3: **for** $a = 1$ to n **do**
4: **if** $M_a = true$ **then**
5: $X_i = MODDEGERI(K_a)$ ▷ Polinomun interpolate edilmesi sırasında tanım kümesi olarak kullanılacak değerler dizisi
6: i = i + 1
7: **end if**
8: **end for**
9: **for** $i = 1$ to n **do**
10: $Y_i = RASTGELESAYIURET()$ ▷ rastgele sayılar mod m' de üretilir, Y_i: Polinomun interpolate edilmesi sırasında değer kümesi olarak kullanılacak değerler dizisi
11: **end for**
12: $P(x) = Interpolate(X_i, Y_i)$ ▷ değeri mod m' de hesaplanır
13: $Z = RASTGELESAYIURET()$ ▷ polinomun değerini hesaplarken kullanılacak mod m' de rastgele sayı üretilir
14: Bob'a Y_i değerleri ve Z değeri gönderilir
15: P_j ▷ BOB' un hesaplayarak ALICE'e gönderdiği değerler dizisi
16: **for** $i = 1$ to j **do**
17: **if** $P_i = P(Z)$ **then** ▷ Gelen değerler arasında P(Z) değeri var mı
18: **return** $true$
19: **end if**
20: **end for**
21: **return** $false$
22: **end function**

Algorithm 2 Bob' un Fonksiyonu

1: **function** POLINOMDEGERLERINIHESAPLA (K_a, L_a, n, m, c, Z) ▷ K_a : gömülü anahtarlar dizisi, L_a : Alice tarafından verilen noktaların dizisi, n : anahtar uzunluğu, m : mod değeri, c : kombinasyon büyüklüğü, Z : polinom değerinin hesaplanacağı nokta
2: C_{pr} = KOMBİNASYON(K_a, n, c) ▷ verilen anahtar uzunluğu ve kombinasyon sayısının hesaplanmış kombinasyon değerlerini tutan dizilerin dizisidir. Her bir kombinasyon alt dizi olarak tutulur.
3: **for** $u = 1$ to p **do**
4: **for** $v = 1$ to r **do**
5: X_v = MODDEGERI(K_{Cpr}) ▷ Polinomu interpolate etmek için tanım kümesinde kullanılacak değerler dizisi
6: $Y_v = L_{Cpr}$ ▷ Polinomu interpolate ederken değer kümesi olarak kullanılacak değerler dizisi
7: **end for**
8: $P_u(x)$ = Interpolate (X_v , Y_v) ▷ değerler mod m' de hesaplanır
9: **end for**
10: Alice'e $P_u(Z)$ değerlerini gönder
11: **end function**

4.2.3 Uygulama görüntüleri

Uygulamamızda 1024 bitlik büyük sayılarla çalışabilmek için GMP [40] kütüphanesini kullandık. C++ ile Code Blocks IDE üzerinde geliştirme yaptık. Uygulamamızdaki algoritmalar bölüm 4.2.2'de listelenmiştir. İki farklı filo için iki ayrı çalıştırılabilen uygulama yazdık. Bu uygulamaların ekran görüntüleri aşağıda listelenmiştir.

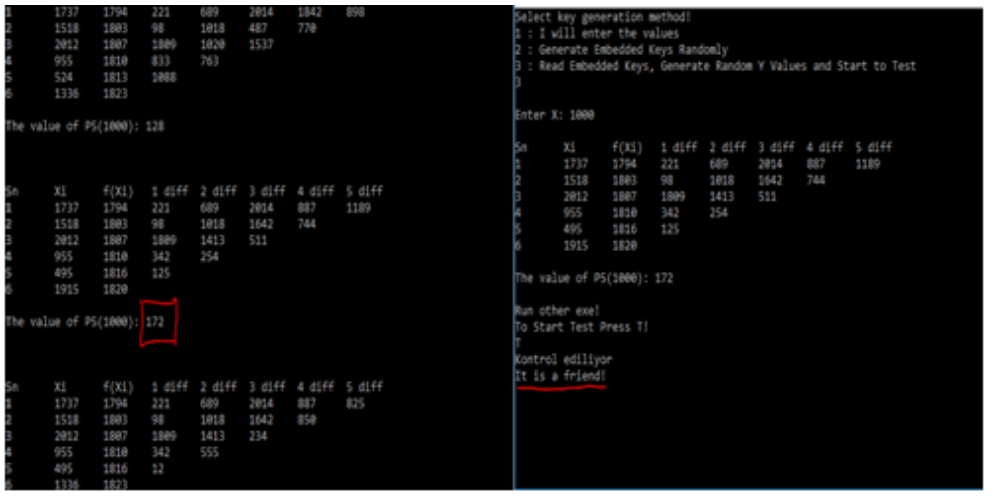
Şekil 4.3'de Filo A uçağı programını çalıştırarak Filo B'ye soracağı $P(X)$ değerini hesaplar. Şekildeki örnekteki $P5(1000)$ değeri 5.dereceden bir polinomda 1000 değerini hesaplattığını gösteriyor. Şekil 4.4'te Filo B'nin, A filosunun göndermiş olduğu Y değerleriyle kombinasyon sonucu kadar ürettiği polinomlar gösterilmiştir. Şekil 4.5'da A filosu B filosundan dönen değerleri test eder. Kendi bulduğu sonuç B filosunun göndermiş olduğu değerlerde var ise dost olarak işaretleme yapar. Eğer yok ise bilinmeyen olarak işaretler.

```
Select key generation method!
1 : I will enter the values
2 : Generate Embedded Keys Randomly
3 : Read Embedded Keys, Generate Random Y Values and Start to Test
3

Enter X: 1000

Sn      Xi      f(Xi)   1 diff  2 diff  3 diff  4 diff  5 diff
1       1737    1794    221     689     2014    887     1189
2       1518    1803    98      1018    1642    744
3       2012    1807    1809    1413    511
4       955     1810    342     254
5       495     1816    125
6       1915    1820

The value of P5(1000): 172

Run other exe!
To Start Test Press T!
```

Şekil 4.3 : Filo A'nın çalıştırdığı program.

```
Sn      Xi      f(Xi)   1 diff  2 diff  3 diff  4 diff  5 diff
1       1737    1794    662     1858    1592    319     897
2       1021    1797    764     134     569     781
3       823     1800    801     1270    1465
4       1518    1803    98      1018
5       2012    1807    1809
6       955     1810

The value of P5(1000): 1176


Sn      Xi      f(Xi)   1 diff  2 diff  3 diff  4 diff  5 diff
1       1737    1794    662     1858    1592    319     135
2       1021    1797    764     134     569     1958
3       823     1800    801     1270    1654
4       1518    1803    98      889
5       2012    1807    1895
6       524     1813

The value of P5(1000): 445


Sn      Xi      f(Xi)   1 diff  2 diff  3 diff  4 diff  5 diff
1       1737    1794    662     1858    1592    319     1775
2       1021    1797    764     134     569     350
3       823     1800    801     1270    16
```

Şekil 4.4 : Filo B'nin çalıştırdığı program.

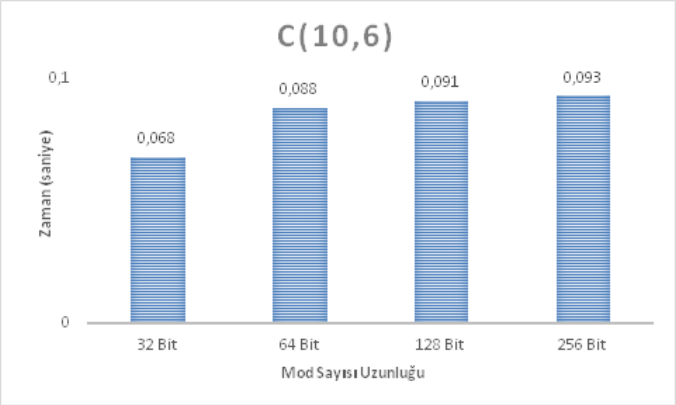


Şekil 4.5 : Filo A'nın Filo B'den dönen sonucu test etme aşaması.

4.3 Ölçümler

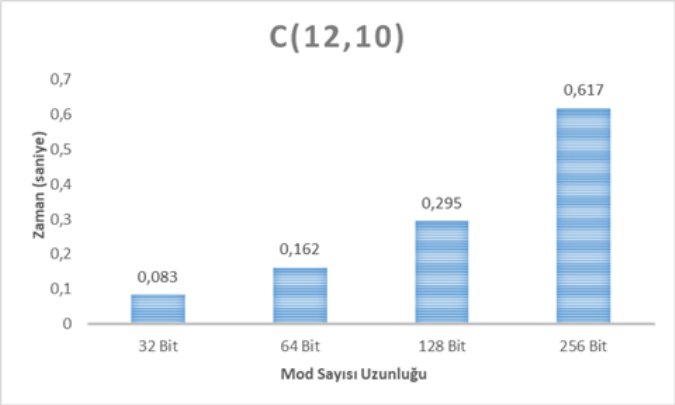
Uygulamamızın büyük asal sayılardaki modlarının ve farklı kombinasyon değerlerindeki sonuçları bu bölümde gösterilmiştir.

Şekil 4.6'de ilgili seçimleri gösteren grafikte sorgulayıcı ve cevaplayıcı tarafta gömülü olan anahtarlar 10 adet değere sahiptir. Bu 10 adet değerin 6 tanesi ortaktır. Sorgulayıcı ve cevaplayıcı için dost-düşman tespitinde geçen toplam süre anahtar değerlerinin uzunluğuna göre değişkenlik göstermekte olup, kullanılan anahtar değeri uzunluğunun toplam süreye etkisinin az olduğu söylenebilir. Burada sorun teşkil edebilecek durum; bu kombinasyon için cevaplayıcı tarafın dönmesi gereken veri seti 210 adet değer içereceğinden ötürü, seçilen küçük modlarda cevaplayıcı tarafın düşman iken kendisini dost olarak tanıtma ihtimali yüksek olacaktır.



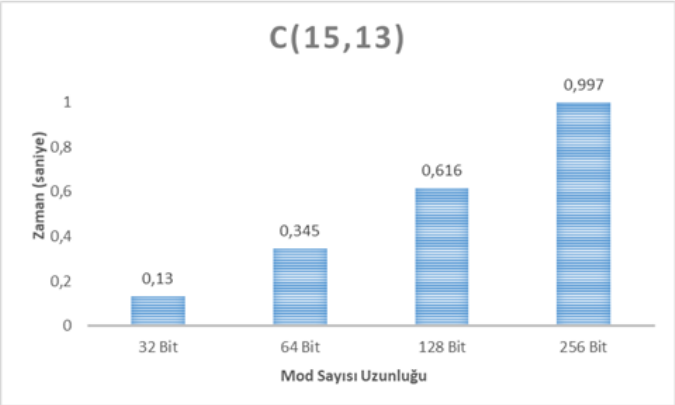
Şekil 4.6 : Onlu anahtar değerin altılı kombinasyonu.

Şekil 4.7'de ilgili seçimleri gösteren grafikte sorgulayıcı ve cevaplayıcı tarafta gömülü olan anahtarlar 12 adet değere sahiptir. Bu 12 adet değerin 10 tanesi ortaktır. Sorgulayıcı ve cevaplayıcı için dost-düşman tespitinde geçen toplam süre anahtar değerlerinin uzunluğuna göre değişkenlik göstermekte olup, kullanılan anahtar değeri uzunluğunun toplam süreye etkisinin olduğu söylenebilir. Burada sorun teşkil edebilecek durum; bu kombinasyon için cevaplayıcı tarafın dönmesi gereken veri seti 66 adet değer içereceğinden ötürü, seçilen küçük modlarda cevaplıyıcı tarafın düşman iken kendisini dost olarak tanıtma ihtimali görece düşük olmasına rağmen yine de düşük olmayacaktır.



Şekil 4.7 : Onikili anahtar değerin onlu kombinasyonu.

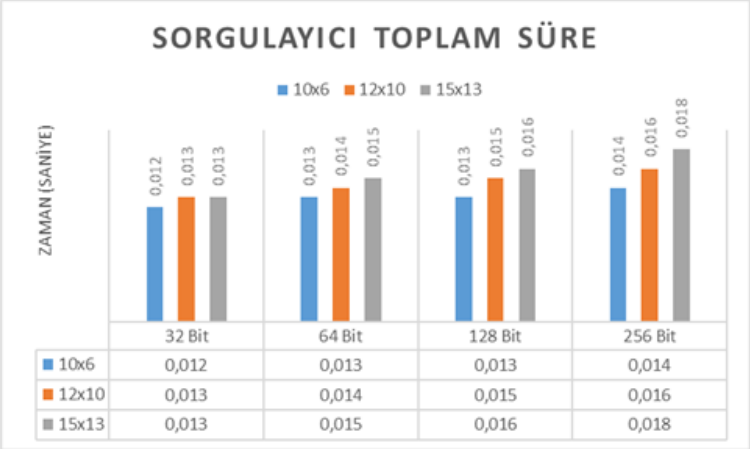
Şekil 4.8'de ilgili seçimleri gösteren grafikte sorgulayıcı ve cevaplayıcı tarafta gömülü olan anahtarlar 15 adet değere sahiptir. Bu 15 adet değerin 13 tanesi ortaktır. Sorgulayıcı ve cevaplayıcı için dost-düşman tespitinde geçen toplam süre anahtar değerlerinin uzunluğuna göre ciddi etkide değişkenlik göstermekte olup, kullanılan anahtar değeri uzunluğunun toplam süreye etkisinin çok fazla olduğu söylenebilir. Burada sorun teşkil edebilecek durum; bu kombinasyon için cevaplayıcı tarafın dönmesi gereken veri seti 105 adet değer içereceğinden ötürü, seçilen küçük modlarda cevaplıyıcı tarafın düşman iken kendisini dost olarak tanıtma ihtimali görece yüksek olacaktır.



Şekil 4.8 : Onbeşli anahtar değerin onüçlü kombinasyonu.

Şekil 4.9'de sorgulayıcı tarafta geçen toplam süre gösterilmiştir. Burada hem seçilen anahtar değerinin uzunluğunun hem de toplam anahtar-ortak anahtar sayısının sonuca büyük oranda etki etmediği gözlenmiştir. Seçilen en küçük mod uzunluğu ve en az anahtar sayısı değeri ile, en büyük mod uzunluğu ve en çok anahtar sayısı değeri

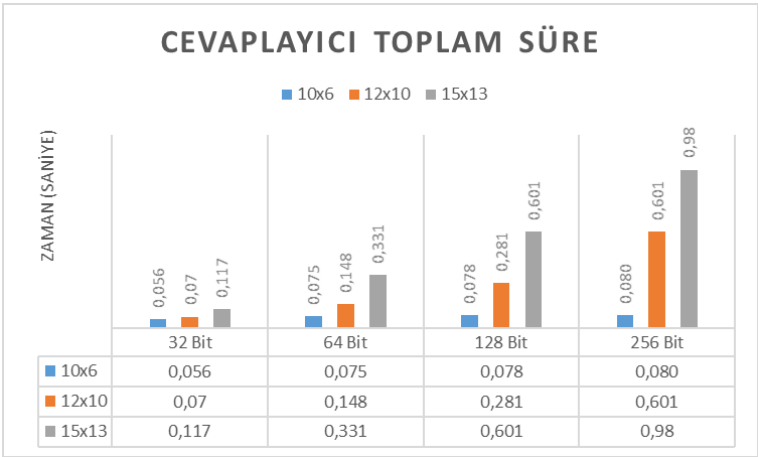
arasında 1'e 1.5 oran vardır. Burada cevaplayıcı taraftan alınan polinom sonuçları 10x6' lık (10 gömülü anahtar, 6 tanesi ortak) anahtar değerlerinde en fazla (210 adet) olsa da, polinom interpolasyonunun daha fazla sayıdaki anahtar değerlerinde daha uzun sürmesi düşünüldüğünde oranın aslında yüksek olmadığı anlaşılacaktır.



	32 Bit	64 Bit	128 Bit	256 Bit
10x6	0,012	0,013	0,013	0,014
12x10	0,013	0,014	0,015	0,016
15x13	0,013	0,015	0,016	0,018

Şekil 4.9 : Sorgulayan tarafta toplam süre.

Şekil 4.10'de cevaplayıcı tarafta geçen toplam süre gösterilmiştir. Burada seçilen anahtar değerinin uzunluğunun da sonuca etki ettiği görülmüştür. Ayrıca toplam anahtar-ortak anahtar sayısının da seçilen mod değeri büyüdükçe, çok daha büyük oranda etki ettiği gözlenmiştir. Seçilen en küçük mod uzunluğu ve en az anahtar sayısı süre değeri ile, en büyük mod uzunluğu ve en çok anahtar sayısı süre değeri arasında 1'e 17.5 oran vardır. Bu oranın bu kadar yüksek çıkması cevaplayıcı tarafta polinom interpolasyonu için hesaplanması gereken polinomun zorluk seviyesinin daha yüksek olması gösterilebilir.



	32 Bit	64 Bit	128 Bit	256 Bit
10x6	0,056	0,075	0,078	0,080
12x10	0,07	0,148	0,281	0,601
15x13	0,117	0,331	0,601	0,98

Şekil 4.10 : Cevaplayan tarafta toplam süre.

4.4 Olasılık Hesaplaması

Olasılık nedir?

Olasılık, bir olayın meyda gelme ihtimalinin ölçümü olarak tanımlanabilir. Bu ölçüm her zaman 0 ile 1 arasında bir değer alır. Ölçüm 0'a yaklaştıkça ilgili olayın olma ihtimali azalıyorken, 1'e yaklaştıkça ilgili olayın olma ihtimali artıyor denilir. Ölçümün 0 olması imkânsızlığı, 1 olması kesinliği belirtir.

Deney: Tekrarlandığı her durumunda farklı sonuçlar elde edilebilen, teorik olarak belirli koşullar altında sonsuz sayıda tekrarlanabilen ve olası sonuçlarının çok iyi tanımlandığı süreçlere deney denir.

Örneklem sonucu: Bir deneyin olası sonuçlarından her bir tanesi örneklem sonucu olarak adlandırılır.

Örneklem uzayı: Bir deneyde bütün örneklem sonuçlarını içeren küme örneklem uzayı olarak adlandırılır.

Olay : Deney sonuçlarından her bir tanesine veya belirli istekleri karşılayan deneyin sonuçlar kümesine de olay denir. Örneğin madeni paranın atılması bir deneydir. Bu madeni para arka arkaya 3 kere atıldığında Y, T, T gelebilir ve bu bizim bir örneklem sonucumuzdur. Bütün örneklem sonuçlarından yani YYY, YYT, YTY, TYY, YTT, TYT, TTY, TTT değerlerinden oluşan kümeye örneklem uzayı denilir. Olay da bir madeni paranın 3 kere atıldığında toplamda 2 kez yazı, 1 kez tura gelmesidir. Bir deneyde n tane olası sonuç olduğu ve bu olası sonuçların her bir tanesinin eşit olasılıklı olarak ortaya çıktığını kabul edelim. Eğer A olarak tanımlamış olduğumuz bir olay, toplam n tane eşit olasılıklı durum içerisinden m tanesinde gerçekleşiyorsa, A olayının olma olasılığı P(A)= m/n olarak ifade edilir.

Bizim önerdiğimiz metottaki olasılık incelemesi

Cevaplayıcı tarafta, polinomu interpolate ederken kullanılmak üzere; x_i değerleri olarak n adet gömülü anahtar değeri ve y_i değerleri olarak da n adet sorgulayıcı taraftan gönderilmiş değer vardır. Cevaplıyıcı, anahtar değerlerinden daha önce üzerinde anlaşılan k sayıda örneklemi ve rastgele sayılar içerisinden bu anahtar değerlere karşılık gelen değerleri kullanarak polinomu interpolate eder. Burada interpolate edilecek $\binom{n}{k} = z$ adet polinom vardır. İnterpolate edilen bu z adet polinomun yine sorgulayıcı tarafından gönderilmiş olan ilgili noktadaki değerleri hesaplanır

ve hesaplanan bu z adet değer sorgulayıcı tarafa gönderilir. Sorgulayıcı taraf da kendi hesaplamış olduğu değer bu z adet değerin içerisinde var mı diye bir arama gerçekleştirir. Bütün bu işlemler $\bmod m$' de hesaplanır. Cevaplayıcı tarafın döndüğü z adet değer de $\bmod m$' de hesaplanır. Burada bir dostun düşman olarak işaretlenme ihtimali bulunmuyorken, bir düşmanın dost olarak işaretlenme ihtimali vardır. Çünkü sorgulayıcı taraf; cevaplayıcı tarafı dost olmasa dahi; z adet gönderdiği değerler içerisinde kendi bulmuş olduğu değer varsa cevaplayıcı tarafı dost olarak işaretler. Bu olayın olma ihtimali de kullanılan mod değeri ile beraber, üzerinde anlaşılmış olan n ve k sayılarına da bağlıdır.

Yukarıdaki olasılık ile ilgili verilen bilgiler ve metotta kullanılan değerler ışığında kabaca hesaplamak gerekirse; sorgulayıcı tarafın cevaplayıcı taraftan $\bmod m$' de z adet değer beklediği durumunda, cevaplayıcı tarafın gönderdiği değerler içerisinde sorgulayıcı tarafın hesapladığı değerin olma ihtimali $P(A) = \frac{z}{m}$'dir. Dolayısıyla z ne kadar küçük, m değeri de ne kadar büyük olursa cevaplayıcı tarafın düşman iken dost olarak tanınma ihtimali bir o kadar küçük olacaktır.

Burada alternatif olarak, sorgulayıcı taraf cevaplayıcı taraftan yukarıdaki tüm süreci birden çok kez (s kez) yapmasını da isteyebilir. Bunu istediği durumda karşı tarafın kendisini düşman iken dost olarak tanıtma ihtimalini de düşürmüş olur. Çünkü cevaplayıcı taraf düşman iken ilk seferde kendisini dost olarak $\frac{z}{m}$ ihtimalle tanıtabilir. İkinci seferde $\frac{z}{m} * \frac{z}{m}$ ihtimalle tanıtabilir. Üçüncü seferde $\frac{z}{m} * \frac{z}{m} * \frac{z}{m}$ ihtimalle tanıtabilir. Yani cevaplayıcı taraf düşman iken süreç s adet işletildiğinde kendisini $(\frac{z}{m})^s$ ihtimalle dost olarak tanıtabilir. Burada s sayısı arttıkça ilgili ihtimalin azalacağı açıkca görülmektedir.

5. SONUÇ VE ÖNERİLER

Bu çalışmada dost uçakların tespit edilebilmesi için yeni bir tanıma şeması önerilmiştir. Hava savunma sistemi için modern şifreleme tekniklerine dayalı yeni bir tanıma şemasıdır. Önerilen yöntem kolayca uygulanabilir ve şifrelenmiş formlarda kodlanmış gizli mesaj alışverişi olmadan eş zamanlı olarak uçak kimlik doğrulaması yapılabilir. Okuyucuya diğer tanıma şemaları aktarılmış ve tanıma sistemlerinin kullandığı algoritmalar incelenmiştir. Sıfır bilgi ispatı algoritması kullanılarak hava taşıtları arasında herhangi bir gizli bilgi paylaşımı (anahtar değer, IFF kod gibi) olmadan dost/düşman tespiti yapılabilmiştir. Yöntemi gerçekleştirmek için, literatürdeki diğer yöntemlerin performansını önemli ölçüde artıran bir tanımlama şeması önerdik. Hava savunma koruma mekanizmasının bütünlüğü de bu tanıma protokolü kullanılarak önemli ölçüde arttırılabilir. Radar istasyonu tarafından tutulacak gizli bilgi yoktur önerdiğimiz sistemde. Radar istasyonları ile uçaklar arasındaki iletişim bağlantılarının güvenli olması gerekmediğinden, geleneksel iletişim bağlantısı şifrelemesi ve anahtar yönetimi ile ilgili işletme maliyeti büyük ölçüde azaltılabilir. Bu araştırma, uçak güvenliği alanında daha fazla araştırma yapmak için yeni zorluklar ve fırsatlar sunuyor. Bunlardan biri, önerilen yöntemi uygulamak ve gerçek ortamlarda test etmektir. Askeri sistem tarafında pratik kullanımda olan güvenlik çözümü doğal olarak sivil güvenlik çözümlerinin de ilgisini çekebilir. Geliştirdiğimiz tanıma şeması hem askeri hem sivil havacılıkta kullanılmasını öngörmekteyiz.

Gelecekte yapılabilecek çalışmalar :

DO-178B standartlarına uygun geliştirilmiş yazılımlar dünyada kabul görmüş yazılımlardır diyebiliriz. Geliştirdiğimiz bu tanıma modelinde kullanılacak yazılım ileriki çalışmalarda DO-178B standartına uygun olabilecek bir şekilde ele alınabilir.

KAYNAKLAR

[1] **Url-1**, Radar System Interfacing, https://www.globalsecurity.org/military/library/policy/navy/nrtc/14089_ch3.pdf, alındığı tarih:12.04.2019.

[2] **Neemat, S. ve Inggs, M.** (2012). Design and implementation of a digital real-time target emulator for secondary surveillance radar / identification friend or foe, *IEEE Aerospace and Electronic Systems Magazine*, *27*(6), ss.17–24.

[3] **ICAO**. ICAO Annex 10 on the Convention on International Civil Aviation Aeronautical Telecommunications Volume IV: Surveillance and Collision Avoidance Systems.

[4] **Url-2**, Lecture 10: traffic alert and collision avoidance system (tcas), https://slideplayer.com/slide/8335852/, alındığı tarih: 15.04.2019.

[5] **Nolan, M.**, (2010). Fundamentals of Air Traffic Control, 5. sürüm.

[6] **Url-3**, (2013), American Institute of Aeronautics and Astronautics. A Framework for Aviation Cybersecurity, https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf, alındığı tarih:12.03.2016.

[7] **CPNI** (August 2012). Cyber Security in Civil Aviation, Centre for the Protection of National Infrastructure, s.2.

[8] **FAA** (2012). Aeronautical Information Manual.

[9] **Strohmeier, M.**, **Schäfer, M.**, **Smith, M.**, **Lenders, V. ve Martinovic, I.** (2016). Assessing the impact of aviation security on cyber power, *2016 8th International Conference on Cyber Conflict (CyCon)*, s.s.223–241.

[10] **Url-4**, GNU Radio, https://gnuradio.org, alındığı tarih: 16.04.2019.

[11] **Strohmeier, M.**, **Schafer, M.**, **Lenders, V. ve Martinovic, I.** (2014). Realities and challenges of nextgen air traffic management: the case of ADS-B, *IEEE Communications Magazine*, *52*(5), ss.111–118.

[12] **TMMOB-EMO** (2014). TMMOB EMO Ankara Şubesi Haber Bülteni 2014/2.

[13] **Ian Moir, A.G.S.**, (2006). Military Avionics Systems, Wiley.

[14] **Wyndham, B.A.** (1988). Secondary Surveillance Radar. M. C. Stevens. Artech House Inc., Norwood. 300 pp. Illustrated. £55.00., *The Aeronautical Journal (1968)*, *92*(919), ss.375–375.

[15] **Simon Kingsley, S.Q.** (1999). Understanding Radar Systems.

[16] **Helliar, R.** Processing and Simulating IFF Radar: A Primer and Review of SPx Software Capabilities.

[17] **Military Agency for Standardization, N.A.T.O.** (1990). Standardization Agreement (STANAG) 4193 PART 1 edition 2 Annex A and appendices, Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders.

[18] **TMMOB-EMO** (2015). TMMOB EMO Ankara Şubesi Haber Bülteni 2015/3.

[19] **Beasley, B.** (2012). Understanding Mode S Technology.

[20] **Cook, E.** (2015). ADS-B, Friend or Foe: ADS-B Message Authentication for NextGen Aircraft, *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, s.ss.1256–1261.

[21] **FAA** (2010). "Automatic Dependent Surveillance- Broadcast (ADS-B) Out Performance Requirements to Support Air Traffic Control (ATC) Service; Final Rule".

[22] **Xu, Y.** (2013/03). TCAS/ ADS-B Integrated Surveillance and Collision Avoidance System, *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering*, Atlantis Press.

[23] **Voles, R.**, (1989), IDENTIFICATION OF FRIEND OR FOE (IFF) SYSTEMS, `https://patents.google.com/patent/US4862176A/en`, United States Patent Number: 4,741,207.

[24] **Ayeh, E. ve Namuduri, K.** (2009). Zero-knowledge proof based node authentication, *University of North Texas, Tech. Rep.*

[25] **McKay, B.D.** (1981). *Practical graph isomorphism*, Dept. of Computer Science, Vanderbilt University.

[26] **Wagner, R.** IFF, combat ID and the information domino effect, *IFF, combat ID and the information domino effect*, Ottawa, ON, Canada.

[27] **Baek, J.**, **Byon, Y.**, **Hableel, E. ve Al-Qutayri, M.** (2013). An Authentication Framework for Automatic Dependent Surveillance-Broadcast Based on Online/Offline Identity-Based Signature, *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, s.ss.358–363.

[28] **El-Badawy, E.A.**, **EL-Masry, W.A.**, **Mokhtar, M.A. ve Hafez, A.S.** (2010). A secured chaos encrypted mode-S aircraft identification friend or foe (IFF) system, *2010 4th International Conference on Signal Processing and Communication Systems*, s.ss.1–6.

[29] **Ammar Alkassar, Christian Stüble, A.R.S.** (2007). Secure object identification: or: solving the Chess Grandmaster Problem, *NSPW '03 Proc. 2003 Workshop New Security Paradigms*, ss.77–85.

[30] **Uriel Feige, A.S.** (1990). Witness Indistinguishable and Witness Hiding Protocols, *In Proceedings of the PPnd Annual Symposium on Theory of Computing (STOC)*, ss.416–426.

[31] **Alkassar, A. ve Stuble, C.** (2002). Towards secure IFF: preventing mafia fraud attacks, *MILCOM 2002. Proceedings*, *2*, ss.1139–1144 vol.2.

[32] **Ikram, N. ve Shepherd, S.J.** (1998). A new approach towards secure IFF technique, *IEEE Military Communications Conference. Proceedings. MILCOM 98 (Cat. No.98CH36201)*, ss.1013–1017 vol.3.

[33] **Shamir, A.** (1985). Identity-Based Cryptosystems and Signature Schemes, *Advances in Cryptology.CRYPTO 1984. Lecture Notes in Computer Science, vol 196. Springer, Berlin, Heidelberg*, ss.47–53.

[34] **C.H.Lin, C.Chang, T.W.R.** (1991). Password authentication using Newton's interpolating polynomials, *Information Systems*, *16*(1), ss.97 – 102.

[35] **Chin-Chen Chang, Ren-Junn Hwang, T.C.W.** (1992). Cryptographic key assignment scheme for access control in a hierarchy, *Information Systems*, *17*(3), ss.243 – 247.

[36] **Chi-Sung Laih, Lein Harn, J.Y.L.** (1989). On the design of a single-key-lock mechanism based on Newton's interpolating polynomial, *IEEE Transactions on Software Engineering*, *15*(9), ss.1135–1137.

[37] **S.Goldwasser, S.Micali, C.R.** (1985). The Knowledge Complexity of Interactive Proof-systems, *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, ss.291–304.

[38] **Goldwasser, S. ve Micali, S.** (1984). Probabilistic Encryprion, *JCSS*, *28*(2).

[39] **H.Aronsson** (1995). Zero Knowledge Protocols and Small Systems, *Department of Computer Science, Helsinki University of Technology*.

[40] **Url-5**, `https://gmplib.org/`, GNU Multiple Precision Arithmetic Library,alındığı tarih: 15.04.2019.

ÖZGEÇMİŞ

Ad Soyad: Buse Tekin Aydın

Doğum Tarihi ve Yeri: 01.07.1992 Ankara

E-Posta: tekinbu@itu.edu.tr

ÖĞRENİM DURUMU:

- **Lisans:** 2015,Hacettepe Üniversitesi,Mühendislik Fakültesi,Bilgisayar Mühendisliği.

MESLEKİ DENEYİMLER VE ÖDÜLLER:

- 2018 yılından itibaren Türk Havacılık ve Uzay Sanayii A.Ş.(TUSAŞ)'da Yazılım Tasarım Mühendisi olarak çalışmaktadır.
- 2018 yılında Monitise firmasında Android Yazılım Geliştirici olarak çalıştı.
- 2015-2017 yılları arasında Yapı Kredi Bankası'nda Yazılım Mühendisi olarak çalıştı.

YÜKSEK LİSANS TEZİNDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

- Aydın T.B,Özdemir E.,Secure Identification Friendly Aircraft, *Congress of Energy, Economy and Security (ENSCON'19)* , Nisan 6-7, 2019 İstanbul, Turkey. (Sunum ve bildiri)
- Aydın T.B,Özdemir E.,Double Layer Security Model for Identification Friend or Foe, *ICAWS 2019 : 21th International Conference on Aerial Warfare and Security* Aug 08-09, 2019 ,New York, USA. (Abstract)