Hava-Hava ve Hava-Yer Taktik Data Link Sistemi için Kriptografi Donanımı

Muhammet Hamdi Yavuz, Osman Buğra Sarıca, Mehmet Haluk Canberi, Alper Kılıç

***Özet*—Geliştirilen "Data Link Tabanlı Dağıtık Gömülü Simülasyon Sistemi" kapsamında muharip hava platformlarının uçuş esnasında havada birbirleriyle ve yer istasyonlarıyla haberleşmeleri gerekmektedir. Haberleşme esnasında askeri açıdan kritik ve gizli bilgilerin paylaşılması gerektiğinden; haberleşmenin güvenilirliğinin sağlanması yani şifrelenmesi gerekliliği ortaya çıkmaktadır. Bu sebeple yüksek başarımlı, esnek ve yüksek güvenilirlikli bir kriptosistem donanımsal olarak FPGA üzerinde gerçeklenmiş ve elde edilen sonuçlar/kazanımlar paylaşılmıştır.**

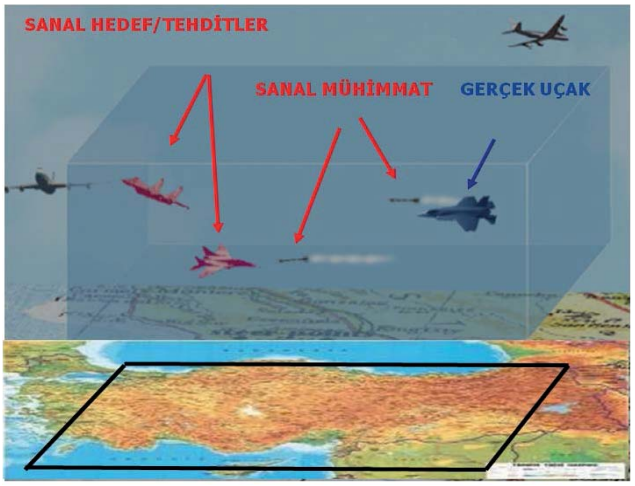
***Anahtar Kelimeler*—aes, data link, fpga, kriptografi, simülasyon**

***Abstract*— Combat aircrafts must communicate with each other and with ground stations during flight within the scope of the project "Data Link Based Distributed-Embedded Simulation System". During communication, because of the transferred data is militarily critical and secret, the necessity of ensuring the reliability of the communication, namely the necessity of encryption of the communication arises. Thus, a cryptosystem with high performance, high reliability and flexibility is implemented on FPGA and the results/benefits of the design are shared.**

***Index Terms*—aes, data link, fpga, cryptography, simulation**

I. GİRİŞ

EĞİTİM ortamı yaratma zorlukları ve fiziksel kısıtlar sebebi ile denenmesi zor olan alt sistemlerin kullanımı, gömülü simülasyon teknolojileri ile sanal olarak gerçekleştirilerek sonuçları görülebilmekte, masraflı olan kullanıcı eğitimlerinin yerini gömülü simülasyon eğitimleri alabilmektedir. Gate Elektronik A.Ş. tarafından geliştirilen Gömülü Eğitim/Simülasyon Sistemi projesi kapsamında; muharip pilotların harbe hazırlık ve harbe hazırlığın devamı niteliğindeki eğitimlerinde yalnızca gerçek uçak kullanılması durumundaki zengin taktik çevre eksikliği ile yer benzetim sistemlerinin kullanımındaki gerçeklik eksiklikleri giderilerek, söz konusu eğitimlerin gerçek uçuş şartlarında, sentetik bir taktik çevre ve sentetik unsurlar oluşturularak yapılması sağlanmaktadır [1]. Şekil 1'de Gömülü Eğitim/Simülasyon Sistemi'nin kavramsal şeması sunulmaktadır. Gömülü Eğitim/Simülasyon Sistemi kapsamında; eğitim senaryosu, pilotun harp zamanında karşılaşabileceği bir taktik durumun, tüm unsurlarını (hız, sürat, tehdit geometrisi yön, irtifa, manevra v.b.), sensör, silah ve meteorolojik şartlar da dahil görüş mesafesi, sistem başarımı v.b.) içerecek şekilde oluşturulabilmektedir. Bununla birlikte hava-hava, hava-yer, yer-hava mühimmatları, elektro-optik mühimmatlar, radar algılayıcıları, IR algılayıcılar, RF karıştırıcılar, karşı tedbir sistemleri (chaff, flare) gibi mühimmat ve algılayıcılar da modellenerek senaryoya dahil edilebilmektedir[1].



Şekil. 1. Gömülü Eğitim/Simülasyon Sistemi Kavramsal Şeması

Gömülü Eğitim/Simülasyon sisteminde, aynı anda yalnızca bir tek pilotun tam olarak eğitimi hedeflenmektedir. Bu projenin devamı niteliğinde olan Data Link Tabanlı Dağıtık Gömülü Simülasyon Sistemi (DLS), Gate Elektronik A.Ş. tarafından, birden fazla hava platformunun aynı senaryo üzerinde eğitimlerini gerçekleştirebilmesi amacıyla geliştirilmektedir. DLS projesi kapsamında, birden fazla muharip uçak, aynı senaryoya dahil olarak birbirleriyle etkileşimli olarak eğitimlerini sürdürebilmektedir. Aynı zamanda; bu uçaklar yer istasyonlarıyla da haberleşerek tüm eğitimin yerde eğitmenler tarafından canlı izlenmesine olanak sağlamaktadırlar. Sözkonusu hava-hava ve hava-yer iletişimi, Gate Elektronik tarafından geliştirilen Data Link Sistemi ile sağlanmaktadır. Data Link ile iletişimde, uçaklar birbirleri ile ve yer istasyonları ile askeri açıdan kritik bilgiler paylaşmaktadır. Bu sebeple; Data Link üzerinden sağlanan veri iletişiminin güvenliğinin sağlanması gerekmektedir. Bu çalışmanın konusu; Data Link sistemi üzerindeki verilerin, sistem mimarisine uygun bir şekilde şifrelenerek güvenli iletişime olanak sağlayacak bir

15.07.2013. Bu çalışma, TÜBİTAK tarafından desteklenen 3110306 numaralı "Data Link Tabanlı Dağıtık Gömülü Simülasyon Sistemi" TEYDEB projesi kapsamında hazırlanmıştır.

Muhammet Hamdi Yavuz, Gate Elektronik A.Ş., Tel: +90 312 257 07 37, e-posta: muhammet.yavuz@gateelektronik.com.tr

Osman Buğra Sarıca, Gate Elektronik A.Ş., Tel: +90 312 257 07 37, e-posta: osman.sarica@gateelektronik.com.tr

Mehmet Haluk Canberi, Gate Elektronik A.Ş., Tel: +90 312 257 07 37, e-posta: haluk.canberi@gateelektronik.com.tr.

Alper Kılıç, Gate Elektronik A.Ş., Tel: +90 312 257 07 37, e-posta: alper.kilic@gateelektronik.com.tr.

kriptografi donanımı tasarımıdır.

II. TEORİ VE SİSTEM MİMARİLERİ

A. *AES Algoritması*

AES (Advanced Encryption Standard) algoritmasından önce var olan DES (Data Encryption Standard) algoritmasının iyi bir algoritma olduğunun kabul edilmesine rağmen; düşük döngü sayısı, düşük şifre parça boyutu sebebiyle ve dönemin meşhur EFF paralel bilgisayarı Deep Crack ile yapılan test saldırılarının sonucunda DES algoritması yerini AES algoritmasına bırakmıştır [2]. Algoritma, NIST (National Institute of Standards and Technology) tarafından düzenlenen yarışma kapsamında Joan Daeman ve Vincent Rijmen tarafından geliştirilmiştir. Doğrulama ve standartlaştırma aşamaları sonrasında NIST, 26 Kasım 2001 yılında FIPS(Federal Information Processing Standard) 197 standardı adı altında AES algoritmasını yayınlamıştır [3]. AES algoritması, 128 bitlik veri bloklarını, 128, 192 veya 256 bitlik genişliklerde şifreleme anahtarları kullanarak şifreleyen bir algoritmadır. Algoritma içerisinde bu veri "state" adı verilen 4x4'lük bayt dizilerinden oluşmaktadır. Algoritmanın dönüşüm işlemleri bu diziler üzerinden uygulanmaktadır [4]. AES Algoritması, "Bayt Değiştirme (SubBytes)", "Satır Kaydırma (Shift Rows)", "Sütun karıştırma (Mix Columns)" ve "Döngü Anahtarı Ekleme (Add Round Key)" adları verilen dört temel dönüşümden oluşmaktadır. Döngü sayısı, anahtar boyutuna bağlı olarak 10, 12 veya 14 olabilmektedir. Şekil 2'de AES şifreleme algoritmasının işleyişi sunulmaktadır [5]. Başlangıçta döngü anahtarı eklendikten sonra, yukarıda ifade edilen dört temel dönüşümü içeren döngü fonksiyonu uygulanır. Son döngüde sütun karıştırma dönüşümü uygulanmaz. Bayt değiştirme dönüşümü, S-kutusu dönüşüm tablosunu kullanarak, 4×4'lük bayt dizilerinin her birini bağımsız olarak, doğrusal olmayan bir şekilde dönüştürme işlemidir. Satır kaydırma dönüşümü, 4×4' lük bayt dizilerinin satırlarını dairesel olarak kaydırma işlemidir. Sütun karıştırma işleminde her bir sütun dört terimli birer polinom olarak düşünülerek sabit bir polinomla çarpılır ve sütunlar dönüştürülmüş olur. Döngü anahtarı ekleme işleminde ise; anahtar genişletme işlemi sonucunda üretilen döngü anahtarlarının, her bir tekrarda diziye özel veya (XOR) işlemi ile katılması söz konusudur.

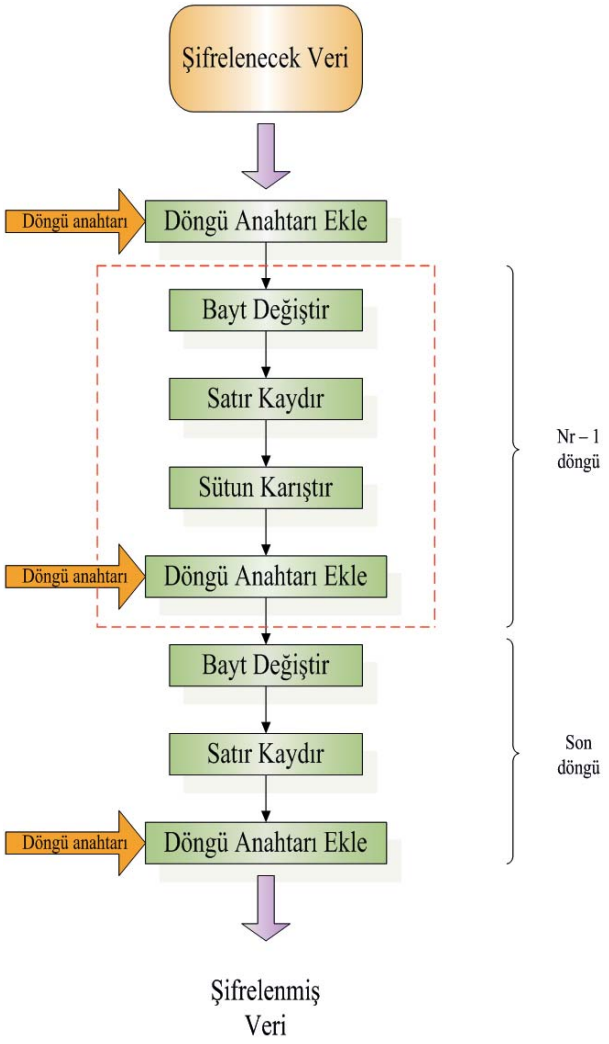
AES şifreleme algoritması ile şifrelenmiş bir veriyi çözmek için AES şifreleme algoritmasında uygulanan dönüşümlerin tersi uygulanmaktadır [6]-[7].

B. *Sahada Programlanabilir Kapı Dizileri (FPGA)*

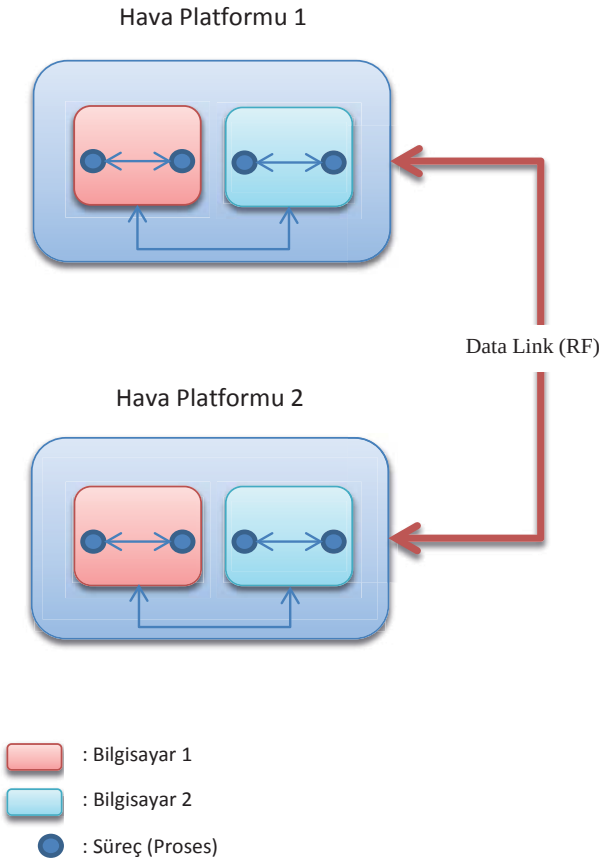
Sahada programlanabilir kapı dizileri (Field programmable gate array), iki boyutlu üreysel mantık hücreleri dizisi ve programlanabilir anahtarları içeren mantıksal aygıtlardır. FPGAlarda mantıksal bir hücre, basit bir işlevi yerine getirmek için programlanabildiği gibi, programlanabilir anahtarlar ise mantıksal hücreler arasındaki ara bağlantıları sağlayacak şekilde düzenlenebilmektedir. Özel bir tasarım, her mantıksal hücrenin işlevinin belirtilmesiyle ve her programlanabilir anahtarın bağlantılarının ayarlanmasıyla gerçeklenebilmektedir. FPGA aygıtları ve geliştirilen donanım tanımlama dilleri sayesinde, üst seviye dillerle, tasarlanan donanımlar tanımlanabilmektedir [8].

C. *Veri Dağıtım Hizmeti (Data Distribution Service)*

Veri Dağıtım Hizmeti (DDS) gerçek zamanlı çalışan dağıtık sistemler için geliştirilmiş bir ara katman hizmetidir. DDS, yüksek başarımlı, güvenilir ve gerçek zamanlı bir yayımcı/abone (publish/subscribe) teknolojisi sunmaktadır. DDS ara katmanı, sağladığı geniş servis kalitesi yönetimi ile gerçek zamanlı ve görev kritik sistemlerin dağıtık ortamdaki ihtiyaçlarını karşılamaktadır. Görev kritik sistemlerde veri aktarımı başarımının öngörülebilir ve deterministik olması beklenmektedir. DDS ara katman mimarisi, DLS projesinde; bu başarımı sağlayarak, süreçler arası haberleşme, bilgisayarlar arası haberleşme ve Data Link vasıtası ile platformlar arası haberleşmede kullanılmaktadır [9].



Şekil. 2. AES Şifreleme Algoritması



Şekil. 3. DLS Haberleşme Mimarisi

D. Data Link Tabanlı Dağıtık Gömülü Simülasyon Sistemi Mimarisi

Birinci bölümde bahsedilen Gömülü Eğitim/Simülasyon sistemlerinin üzerinde çalıştığı hava platformlarının haberleşmesi Data Link ile sağlanmaktadır. Her bir hava platformunun üzerinde iki adet yüksek başarımlı bilgisayar bulunmaktadır. Bu bilgisayarlar hem platform içerisinde birbirleriyle, hem de platformlar arası diğer bilgisayarlar ile haberleşmekte, ayrıca her bir bilgisayar üzerinde çalışan süreçler birbirleri ile haberleşmektedirler. Bahsi geçen haberleşme mimarisi, DDS ara katman mimarisi kullanılarak gerçekleştirildiğinden; bilgisayar içi, platform içi ve platformlar arası haberleşmede yalnızca fiziksel katman tanımlaması değişerek, bellek, Ethernet ya da RF (radio frequency) olabilmektedir[9]. Şekil 3'te DLS haberleşme mimarisi sunulmaktadır.

Muharip hava platformları arasındaki iletişimde, askeri açıdan kritik bilgilerin aktarılması gerektiği için, söz konusu platformlar arasındaki ver iletişiminde bir şifreleme sistemi gereksinimi ortaya çıkmaktadır. Şekil 3'te kırmızı hatla gösterilen iletişim hattı, Data Link kullanılarak radyo dalgaları ile sağlanmaktadır. Bu kırmızı iletişim hattından akan her türlü bilginin gizliliği sağlanmalı, dolayısıyla bir platformdan öteki platforma, bir platformdan yer istasyonuna veya yer istasyonundan bir platforma gönderilecek her türlü veri, kırmızı hatta girmeden önce şifrelenmeli ve alıcı tarafta kırmızı hattan çıktıktan sonra geri çözülmelidir. Güvenli veri ile güvensiz veri soyutlamasının tam anlamıyla yapılabilmesi için; her platformda, görev bilgisayarı ile Data Link anteni arasında şifreleme/çözme (encryption/decryption) işlemlerini yürütecek bir kriptografi donanımına ihtiyaç duyulmaktadır.

III. KRİPTOGRAFİ DONANIMI

Hava-hava, have-yer ve yer-hava Data Link iletişiminde askeri kritik/gizli verilerin güvenli ileitişimini sağlamak üzere bir kriptosistem gerekmektedir. Bu kriptosistemin; uygun bant genişliğinde, güvenli, sürdürülebilir, yüksek başarımlı ve diğer sistem/alt sistemlerden yalıtılmış olarak çalışabilmesi amacıyla yazılımsal çözümden ziyade donanımsal bir çözümün daha uygun olacağı öngörülerek, tasarlanan kriptosistem FPGA üzerinde gerçeklenmiştir.

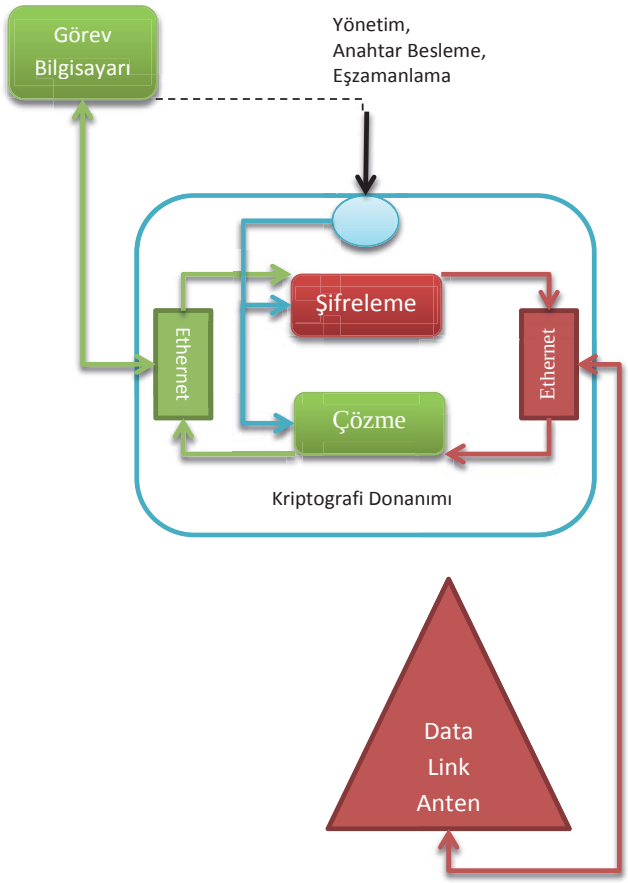
Söz konusu kriptografi donanımı; muharip hava platformunun görev bilgisayarından gelen verileri şifreleyip Data Link antenine, diğer muharip hava platformuna veya yer istasyonuna göndermek üzere iletmekle ve bunun tersi olarak Data Link anteninden gelen verileri çözüp görev bilgisayarına iletmekle yükümlüdür. Bahsi geçen kriptografi donanımının yapısı şekil 4'te sunulmaktadır.

FPGA üzerinde gerçeklenen kriptografi donanımı, veri alış-verişinde Ethernet arayüzünü kullanmaktadır. Donanımın üzerinde iki adet Ethernet arayüzü bulunmaktadır. Bunlardan bir tanesi görev bilgisayarı ile veri alış-verişini sağlarken diğeri Data Link ile veri alış-verişini sağlamaktadır. Şekil 4 üzerinde, yeşil renk ile gösterilen hatlar şifrelenmemiş veri akışını, kırmızı ile gösterilen hatlar ise şifrelenmiş veri akışını ifade etmektedir. Buna göre; görev bilgisayarından, başka bir muharip hava platformunun görev bilgisayarına veya yer istasyonuna gönderilmek istenen veri öncelikle Ethernet arayüzünden kriptografi donanımına iletilir. Uygun zamanlama sağlanacak şekilde bu veriler arabellekte (buffer) tutularak şifreleme birimine iletilir. Burada şifrelenen veri uygun zamanlama için arabellekte biriktirilerek ikinci Ethernet arayüzü yardımıyla Data Link antenine iletilir. Burada radyo dalgalarına çevrilen veri diğer platforma veya yer istasyonuna iletilir. Tersi durumda ise; platforma Data Link vasıtasıyla gelen veri Ethernet arayüzüyle alındıktan sonra arabellekte bekletilerek çözme birimine ulaştırılır. Çözme biriminde şifrelenmiş veriden iletilmek istenen veri elde edilerek arabelleğe ve oradan da Ethernet arayüzü vasıtasıyla görev bilgisayarına aktarılır. Ethernet veri akışının üst seviye görünümü şekil 5'te sunulmaktadır.

A. Şifreleme Algoritmasının Gerçeklenmesi

Sistemde kullanılacak şifreleme algoritması AES-256 olarak seçilmiştir. Data Link için bant genişliği DLS sistem mimarisinin elverdiği ölçüde yaklaşık 6 Mbit/s'dir. DLS'nin esnek yapısı sayesinde, mesafe değiştikçe bant genişliği en uygun seviyeye getirilebilmektedir. Bu sebeple; göreceli olarak çok yüksek bant genişliklerine ihtiyaç duyulmaması hesaba katılarak donanım düşük frekansta çalıştırılarak uçak üzerinde oldukça önemli bir konu olan güç tüketiminin de daha uygun bir seviyeye getirlmesi sağlanabilmektedir.

AES-256 algoritması FPGA üzerinde gerçeklenirken, bayt değiştirme dönüşümünü için 16 adet özdeş S-kutusu (S-box)



Şekil. 4. Kriptografi Donanımı Yapısı

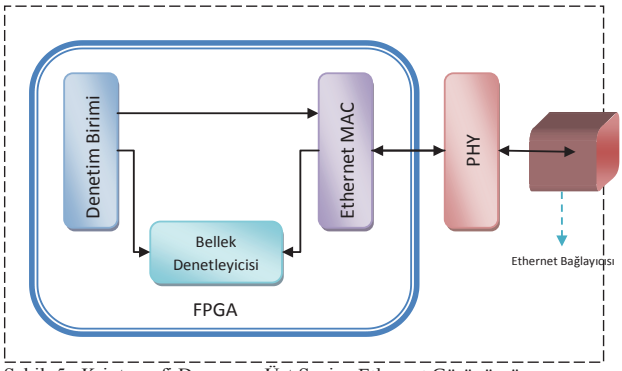
paralel olarak kullanılmıştır. Her bir S-kutusu, FPGA içerisinde birer ROM olarak gerçeklenmiştir. Bu sayede; 128 bitlik bir veri için bayt değiştirme işleminin yalnızca bir saat vuruşu kadar zaman alması sağlanmıştır. Aynı şekilde satır kaydırma işlemi de her bir döngü kütüğü (block) için bir saat vuruşunda yapılabilmektedir. Sütün karıştırma işleminde ise saatten bağımsız bir donanım tasarlanmıştır. Bu dönüşüm, saatten bağımsız olarak gerçekleştirilen en karmaşık bileşen olduğundan, tüm donanımın frekans kısıtının belirlenmesinde önemli rol oynamaktadır. Yalnızca anahtar değişikliği olacağı zaman çalışacak olan anahtar genişletme birimi de aynı paralellikle FPGA üzerindeki mevcut alan gözetilerek tasarlanmıştır [10].

B. Anahtar Yönetimi

Sistemde kullanılacak 256 bitlik anahtarlar iki farklı şekilde elde edilebilmektedir.

Bunlardan ilkinde; kriptografi donanımı üzerinde bulunan seri arayüz kullanılarak, sistemin kullanacağı anahtarlar ve varsa bu anahtarların kullanılacağı zaman bilgileri aktarılır. Bu bilgiler uçuş öncesinde bir USB depolama aygıtına aktarılarak pilota veya diğer yetkili uçuş personeline ilgili sokete takması amacıyla, yetkili kişiler tarafından, yetkili donanımlar kullanılarak güvenli bölgede oluşturularak verilir. Anahtarlar her bir unsurla (diğer hava platformları ve yer istasyonları) haberleşmek için farklı farklı olabileceği gibi, tüm ağda kullanılacak tek bir anahtar da olabilmektedir. Anahtarlar uçuş esnasında pilot isteğine bağlı olarak devingen bir şekilde değişebilmekte veya öntanımlı zaman verileri kullanılarak uygun zamanda sistem tarafından değiştirilebilmektedirler. İstendiği takdirde; bu devingen anahtar değişim kontrolü, görev bilgisayarı üzerindeki yazılım tarafından da, uçuş esnasında elde edilen çeşitli değişkenler yardımıyla, değiştirilebilmektedir.

İkinci yöntemde ise anahtar belirleme amacıyla, Diffie-Hellman protokolü kullanılmaktadır [11]. Bu sayede; muharip hava platformları ve yer istasyonları, güvensiz bir kanal üzerinden devingen olarak güvenli birer anahtar oluşturabilmektedirler. Bu durumda da anahtar zamanlama yönetimi diğer durumla aynı özelliklere sahip olup, ister öntanımlı olarak ister pilot kararı veya yazılım kararıyla yapılabilinmektedir.



Şekil. 5. Kriptografi Donanımı Üst Seviye Ethernet Görünümü

Anahtar girdisinin, sistem yönetiminin ve zamanlama denetiminin yapılabileceği arayüz ve ilgili hatlar şekil 4'te mavi renkle işaretlenmiştir. Kriptografi donanımının her türlü denetimi, uçuş esnasında pilot tarafından da MFD (Multi Function Display) sayfaları yardımıyla yapılabilmektedir.

IV. SONUÇ

AES algoritmasının donanımsal gerçeklemesi yapılırken düşük frekansta yüksek hız kısıtı gözetilmiştir. Boru hattı mimarisiyle paralel olarak tasarlanan donanım, düşük frekansta gereksinimlerinin çok üzerinde bir bant genişliğiyle şifreleme/çözme yapabilme yeteneğine sahip olduğundan, uçak üzerinde en düşük seviyede tutulması gereken güç tüketimi yönünden oldukça olumlu bir başarıma sahip olabilmektedir.

Kriptografi donanımının gerçeklenmesi sonucunda, 16 MHz gibi düşük bir saat sıklığı kullanılarak yaklaşık olarak 120 Mbit/s veri akış hızına ulaşılmıştır. Şifreleme ve çözme donanımı, 10Gbit/s'den daha fazla bir bant genişliğine sahip olması gerekmeyeceği için, FPGA üzerinde oldukça düşük bir alana sahip olmaktadır. Bu sebeple sistem, daha düşük maliyetli FPGAlar üzerinde de rahatlıkla gerçeklenebilmektedir. AES algoritmasının farklı FPGAlar üzerinde veri akış hızları ve kapladığı alanlar Tablo 1'de sunulmaktadır.

Tablo 1'de görüldüğü üzere; göreceli olarak düşük maliyetli bir FPGA (Cyclone III EP3C16F256C8N) oldukça düşük bir frekansta (16MHz) kullanılarak istenilen veri akış hızından daha yüksek bir veri akış hızı sunmaktadır. Saniyede 1 Gb'den daha yüksek veri akış hızları istendiği

TABLO I
AES-256 GERÇEKLEMESININ FARKLI FPGALAR ÜZERINDEKI DEĞERLERI

FPGA	Frekans (MHz)	Kapladığı Alan (%)	Veri Akışı (Mb/s)
Cyclone III EP3C16F256C8N	118.45	14	891.86
Spartan III XC3S2000-5	85.80	< 5	646.02
Virtex 6 XC6VLX550T-2	368.84	< 1	2777.15
Cyclone III EP3C16F256C8N	16	14	120.47

durumda ise; donanım tasarımında ve tanımlamalarında herhangi bir değişiklik yapılmaksızın yalnızca FPGA değiştirilerek (örneğin Virtex 6 XC6VLX550T-2 kullanılarak) istenen veri akış hızları sağlanabilmektedir. Tablo 2'de, yapılan FPGA gerçeklemesinin diğer çalışmalarla karşılaştırılması sunulmaktadır.

TABLO II
AES-256 GERÇEKLEMESININ FARKLI ÇALIŞMALAR İLE KARŞILAŞTIRILMASI

Gerçekleme →	Good [12]	Chodowiec [13]	Rouvroy [14]	Bu Çalışma
FPGA	XC2S15-6	XC2S30-6	XC3S50-4	XC3S2000-5
Frekans (MHz)	67	60	71	85.8
Veri Akışı (Mb/s)	2.2	166	208	646

Sonuç olarak DLS projesi kapsamında kriptografi donanımından beklenen bant genişliği ve frekans değerleri sağlanmakta ve esnek tasarımı sayesinde çok geniş bir aralıkta bu değerlerle oynanabilmektedir

KAYNAKLAR

[1] Kılıç, A., Canberi H., "Muharip Hava Platformları için Gömülü Eğitim/Simülasyon Sistemi", Savunma Teknolojileri Kongresi, SAVTEK, 2012.
[2] Forte, D., The future of the advanced encryption Standard, Network Security, 1999(6), 10-13, 1999.
[3] National Institute of Standards and Technology, Advanced Encryption Standard, FIPS PUB, 197, USA, 2001.
[4] Bruen, A. A., Forcinito, M. A., Cryptography, Information Theory, and Error-Correction : A Handbook fort he 21st Century, Wiley-Interscience, USA, 2005.
[5] Yavuz, M.H., Ergin, O., Verileri Nota Kullanarak Şifreleme ve Ses Dosyası İçerisine Gizleme, 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara", 2008.
[6] Advanced Encryption Standard, Federal Information Processing Standards Publication 197, November, 2001.
[7] S. M. Yoo, D. Kotturi, D. W. Pan, J. Blizzard, "An AES crypto chip usinga high-speed parallel pipelined architecture", Microprocessors and Microsystems, 29(7), pp. 317-326, 2005.
[8] Chu, P.P., FPGA Prototyping by Verilog Examples, Wiley & Sons, New Jersey, 2008.
[9] Türkay, K. D., Canberi, M. H., Kılıç, A., "Görev Kritik Sistemler Açısından DDS Arakatman Mimarisinin Performans Analizi", 5. Ulusal Savunma Uygulamaları Modelleme ve Simülasyon Konferansı, Ankara, 2013.
[10] Yavuz, M. H., "Müzikle Şifreleme-Veri Gizleme Sistemi Tasarımı ve Gerçaklenmesi", Yüksek Lisans Tezi, TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara, 2010.
[11] Diffie, W., Hellman, M. E., New directions in cryptography, IEEE Transactions on Information Theory, 22(6), 644-654, 2006.
[12] Good, T., Benaissa, M., AESon FPGA from the Fastest to the Smallest, Cryptographic Hardware and Embedded Systems (CHES 2005), 3659, 427-440, 2005.
[13] Chodowiec, P., Gaj, K., Very Compact FPGA Implementation of the AES Algorithm, Cryptographic Hardware and Embedded Systems, 2779, 319-333- Springer-Verlag, 2003.
[14] Rouvroy, G., Standaert, F. X., Quisquater, J. J., Legat, J. D., Compact efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications, Procedings of the International Conference on Information Technology: Coding and Computing 2004 (ITCC '04), 2, 583-587, 2004