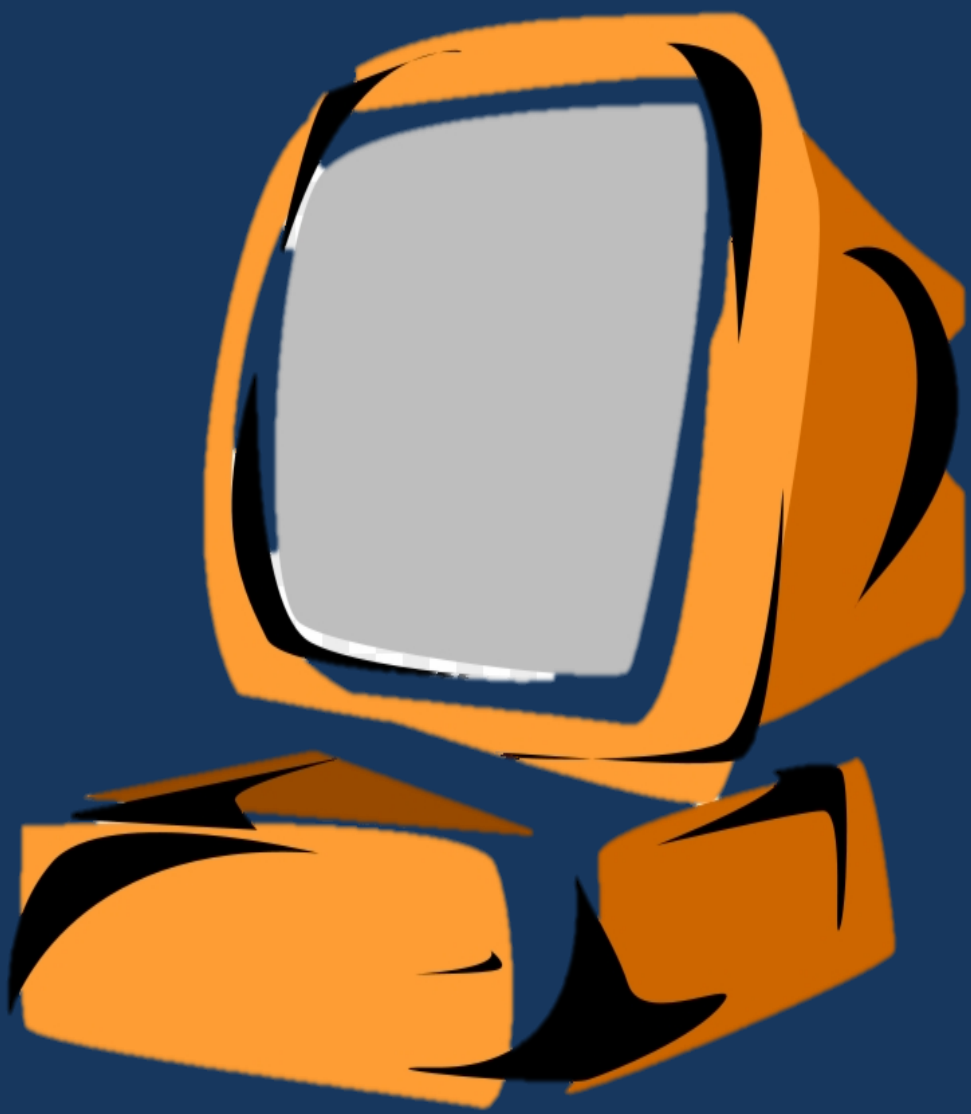
BİLGİSAYAR MÜHENDİSLİĞİ ÇALIŞMALARI-1

Editör
Dr. Süleyman ADAK



BİLGİSAYAR MÜHENDİSLİĞİ ÇALIŞMALARI-1

EDİTÖR

Dr. Öğr. Üyesi Süleyman ADAK

YAZARLAR

Doç. Dr. Cemil İNAN
Dr. Hasan CANGİ
Dr. Öğr. Üyesi Süleyman ADAK
YL.Öğrencisi, Hanifi TOPRAK
Dr.Öğr.Üyesi Süleyman KARDAŞ
Öğr.Gör.Hüseyin ŞAHİN
Doç.Dr.Tuğrul OKTAY
Dr.Ögr.Üyesi Mehmet KONAR
Lec. Oguz KOSE
Assoc. Prof. Tugrul OKTAY
Dr. Öğr. Üyesi Süleyman KARDAŞ
YL. Öğrencisi Roda KIZIL

İKSAD Publishing House

Institution of Economic Development and Social Researches Publications® (The Licence Number of Publicator: 2014/31220)
TURKEY
TR: +90 342 606 06 75
e mail: uluslararasikitap@gmail.com
www.iksad.net
It is responsibility of the author to abide by the publishing ethics rules. Iksad Publications – 2020©
ISBN: 978-625-7914-46-8

March / 2020 Ankara / Turkey

İÇİNDEKİLER

Editörden

Önsöz ……..i

Bölüm 1

HANDS ON MATH
READY TO USE GAMES & ACTIVITIES FOR GRADES (4-8)

Doç.Dr.Cemil İNAN.....Sayfa 1

Bölüm 2

2. KATMAN İÇ AĞ SALDIRILARI ve ÖNLEMLER

YL. Öğrencisi Hanifi TOPRAK
Dr. Öğr.ÜyesiSüleyman KARDAŞ.....Sayfa 16

Bölüm 3

KARARLILIĞIN ELEKTRİK DEVRELERİNDE BİLGİSAYAR DESTEKLİ ANALİZİ

Dr. Hasan CANGİ
Dr. Öğr. Üyesi Süleyman ADAK
Doç. Dr. Cemil İNAN.....Sayfa38

Bölüm 4

DÖNER KANATLI HAVA ARAÇLARININ UÇUŞ PERFORMANS OPTİMİZASYONU

Öğr. Gör. Hüseyin ŞAHİN
Doç. Dr. Tuğrul OKTAY
Dr. Ögr. Üyesi Mehmet KONAR.....Sayfa 52

Bölüm 5

THE EFFECT OF DIFFERENTIAL MORPHING ON THE HOVER FLIGHT IN QUADCOPTER

Lec. Oguz KOSE
Assoc. Prof. Tugrul OKTAY.....Sayfa 59

Bölüm 6

BLOKZİNCİRDE İMZALAMA ALGORİTMALARI

YL. Öğrencisi Roda KIZIL
Dr. Öğr. Üyesi Süleyman KARDAŞ.....Sayfa 73

BÖLÜM1

HANDS ON MATH
READY TO USE GAMES & ACTIVITIES
FOR GRADES (4-8)

Doç. Dr. Cemil İNAN

HANDS ON MATH

READY TO USE

GAMES & ACTIVITIES FOR GRADES (4-8)

Cemil İNAN
Doç. Dr.,Mardin Artuklu Üniversitesi
İktisadi ve İdari Bilimler Fakültesi
İşletme Bölümü

KİTAP İNCELEMESİ

HANDS ON MATH

READY TO USE GAMES & ACTIVITIES FOR GRADES (4-8)

Yazarlar

FRANCES M. THOMPSON

Bu çalışmada yazarlığını Francesb M. Thompson tarafından yazılan "Handa On Math ready to use Games & Activities for Grades" isimli kitabın incelenmesi yapılmıştır. Bir kitap eleştirisi olarak yapılan bu incelemede kitabın biçimsel ve içerik yönlerine ağırlık verilmiştir.

Yüksek öğretim matematik programlarının temel amacı; matematik kavramları ve aralarındaki ilişkileri kurabilecek derinlemesine anlayabilecek ve başta mühendislik dalları olmak üzere bütün uygulamalıbilimlerde başarı ile uygulayabilecek elemanlar yetiştirmektir. Bu amaç bir ülkenin kalkınmasının da temel taşıdır.Öğrenciler orta öğretimden itibaren tümden gelimci anlayışla kavramları anlamadan sadece hafızada tutmaya çalıştıkları bu duruma kısmen uygulanan sınav sistemlerinin neden olduğu söylenebilir.. Öğrencileri alıştıkları öğrenme sitilinden kavram ve işlem bütünlüğü içinde eğitmek uzun zaman

almaktadır. Öğrencilerin geliştirdiği yanlış anlamaları ve kavram yanılgılarını belirlemek ve bu kavram yanılgılarını ortadan kaldırmak için matematik eğitimcilerinin yoğun çalıştıkları ve yayınlar yaptıkları bilinmektedir. Bu tür çalışmaların yanında öğrencilerin hazır bir cebirsel problemi çözme eğiliminde olduğu fakat problemler sözel olarak verildiğinde matematik cümlesini düzenlemede ve çözmede zorluklarla karşılaştıkları yapılan sınavlardan ve uygulamalardan anlaşılmaktadır.

Bunun nedeni olarak ilköğretim yıllarında öğrencilerin matematik kavramları derinlemesine anlamadıkları yada anlatılamadığı anlaşılmaktadır Bu konuda öğrencilerimize destek amacı ile yerli ve yabancı ilköğretim matematik kitapları tarandı bu kitapların bir öncelik sırasına göre incelenip tanıtılması düşünüldü. Hangi kitap ve neden seçildiği konusu önemli olduğundan öncelikle ilköğretime yönelik yabancı kaynaklar taranırken bol çalışma yapraklı ve uygulamalı , istenen tüm konuları kapsayan bir kitap olduğu için Handa On Math ready to use Games & Activities for Grades seçilmiştir

İncelenen bu kitapta; temel matematik kavramları etkinliklerle güçlendirildiğ görülmektedir Kitap dili İngilizce olmasına rağmen basit anlaşılır bir dille yazılmıştır. Bu kitabın incelenmesinden sonra araştırmacılara bu eseri çevirme ve literatürümüze kazandırma fırsatı da vermektedir Bu kitabın matematik alanında çalışan başta akademisyenlere, öğretmenlere ve özellikle öğrencilere faydalı olabileceği düşünülmektedir.

Bu kitap Handa On Math ready to use Games & Activities for Grades kitabı ilköğretimde 4-8 sınıflar için düzenlenmiştir. Öğrencilerinin gelişmesini sağlamak ve matematik kavramlarını anlama yetenekleri geliştirmek için tasarlanmıştır. Çoğu matematik ders kitapları konuyu karışık sistemli olmayan bir şekilde sunmakta ve, öğrenciyi zorlamaktadır.İncelenen kitap matematik ders kitaplarına ek olarak kullanılabilecek bir şekilde sunulmuştur. Handa On Math ready to use Games & Activities for Grades incelenip uygulanırsa öğrencilerin başarıları artacağı söylenebilir Bu kitapta

1.Kolayca anlaşılır terimlerle özlü örnekler verilmiştir.

2.Etkinliklerle konunun anlaşılması desteklenmiştir

3.Çalışma yaprakları ile öğrencinin uygulama ve kendi başına konuyu tekrar etmesi sağlanmıştır.

Bu kitabın amacı, öğrencinin matematik kavramları ve işlemlerini yapabilme yeteneğine olan güvenini arttırmaktır. Eğitimcilere düşen, temel İngilizce biraz zaman ve çaba harcamaktır. Bunun sonucunda kazanacağı yetenek çok değerli olabilecektir.

Bu çalışmada "Handa On Math ready to use Games & Activities for Grades" isimli kitabın eleştirel incelemesi yapılmıştır. Kitap sekiz bölüm ve toplam 515 sayfadan oluşmaktadır. Bu kitap Frances M. Thompson tarafından yazılan ve The Center For Applıed Research In Educatıon-USA yayın evi tarafından yayınlanan kitaba internet üzerinden ulaşılabilmektedir. Kitap geniş bir açıklayıcı önsözle başlamakta kullanma talimatları yanında kitaba beklenen öğrenme beklentilerini de eklenmiştir. Kitabı eleştirel gözle incelemeye başlayabiliriz. bilimlerde başarı ile uygulayabilecek elemanlar yetiştirmektir. Bu amaç bir ülkenin kalkınmasının da temel taşıdır.Öğrenciler orta öğretimden itibaren tümden gelimci anlayışla kavramları anlamadan sadece hafızada tutmaya çalıştıkları bu duruma kısmen uygulanan sınav sistemlerinin neden olduğu söylenebilir.. Öğrencileri alıştıkları öğrenme sitilinden kavram ve işlem bütünlüğü içinde eğitmek uzun zaman almaktadır. Öğrencilerin geliştirdiği yanlış anlamaları ve kavram yanılgılarını belirlemek ve bu kavram yanılgılarını ortadan kaldırmak için matematik eğitimcilerinin yoğun çalıştıkları ve yayınlar yaptıkları bilinmektedir. Bu tür çalışmaların yanında öğrencilerin hazır bir cebirsel problemi çözme eğiliminde olduğu fakat problemler sözel olarak verildiğinde matematik cümlesini düzenlemede ve çözmede zorluklarla karşılaştıkları yapılan sınavlardan ve uygulamalardan anlaşılmaktadır. Bunun nedeni olarak ilköğretim yıllarında öğrencilerin matematik kavramları derinlemesine anlamadıkları yada anlatılamadığı anlaşılmaktadır Bu konuda öğrencilerimize destek amacı ile yerli ve yabancı ilköğretim matematik kitapları tarandı bu kitapların bir öncelik sırasına göre incelenip tanıtılması düşünüldü. Hangi kitap ve neden seçildiği konusu önemli olduğundan öncelikle ilköğretime yönelik yabancı kaynaklar taranırken bol çalışma yapraklı ve uygulamalı , istenen tüm konuları kapsayan bir kitap olduğu için Handa On Math ready to use Games & Activities for Grades seçilmiştir

İncelenen bu kitapta; temel matematik kavramları etkinliklerle güçlendirildiğ görülmektedir Kitap dili İngilizce olmasına rağmen basit anlaşılır bir dille yazılmıştır. Bu kitabın incelenmesinden sonra araştırmacılara bu eseri çevirme ve literatürümüze kazandırma fırsatı da vermektedir Bu kitabın matematik alanında çalışan başta

akademisyenlere, öğretmenlere ve özellikle öğrencilere faydalı olabileceği düşünülmektedir.

Bu kitap Handa On Math ready to use Games & Activities for Grades kitabı ilköğretimde 4-8 sınıflar için düzenlenmiştir. Öğrencilerinin gelişmesini sağlamak ve matematik kavramlarını anlama yetenekleri geliştirmek için tasarlanmıştır. Çoğu matematik ders kitapları konuyu karışık sistemli olmayan bir şekilde sunmakta ve, öğrenciyi zorlamaktadır.İncelenen kitap matematik ders kitaplarına ek olarak kullanılabilecek bir şekilde sunulmuştur. Handa On Math ready to use Games & Activities for Grades incelenip uygulanırsa öğrencilerin başarıları artacağı söylenebilir Bu kitapta

1.Kolayca anlaşılır terimlerle özlü örnekler verilmiştir.

2.Etkinliklerle konunun anlaşılması desteklenmiştir

3.Çalışma yaprakları ile öğrencinin uygulama ve kendi başına konuyu tekrar etmesi sağlanmıştır.

Bu kitabın amacı, öğrencinin matematik kavramları ve işlemlerini yapabilme yeteneğine olan güvenini arttırmaktır. Eğitimcilere düşen, temel İngilizce biraz zaman ve çaba harcamaktır. Bunun sonucunda kazanacağı yetenek çok değerli olabilecektir.

Bu çalışmada "Handa On Math ready to use Games & Activities for Grades" isimli kitabın eleştirel incelemesi yapılmıştır. Kitap sekiz bölüm ve toplam 515 sayfadan oluşmaktadır. Bu kitap Frances M. Thompson tarafından yazılan ve The Center For Applıed Research In Educatıon-USA yayın evi tarafından yayınlanan kitaba internet üzerinden ulaşılabilmektedir. Kitap geniş bir açıklayıcı önsözle başlamakta kullanma talimatları yanında kitaba beklenen öğrenme beklentilerini de eklenmiştir. Kitabı eleştirel gözle incelemeye başlayabiliriz.

BİRİNCİ BÖLÜM: SAYI VE SAYI İLİŞKİLERİ

Bu bölümde; sayılar, sayılarda büyüklük küçüklük, kesirler ve kesirlerde karşılaştırma, sayılarda yuvarlamaya oyun etkinlikleri. Ondalık sayılar ve basamak kavramı, yüzdelik ve bunlar arasındaki ilişkiler ve denk kesirler

oran ve orantı kavramları etkinliklerle ve çalışma yaprakları ile işlenmiştir. Bol örnek olmasına rağmen çalışmanın kapasitesi bakımından önemli bir kaçtan örnek inceleyelim.

Hangisi daha büyük etkinliğinde, renkli kalemler kullanılarak sayılar büyüklüğüne göre tablolara yazdırılır böylece basamak kavramına geçiş yapılır. Basamaklar ve ondalık basamaklar etkinliklerle ve çalışma yaprakları ile işlenmektedir. Oyun çarkları ile basamak kavramı ve sayılar arasındaki ilişki pekiştirilir. Sayılarda yuvarlama çalışmaları tablolar üzerinde ve gruplara ayırarak yapılmaktadır. Kesirler konusunda yarım, çeyrek kavramlarından sonra bir tam kâğıt eşit parçalara bölünerek her bir parçanın bütün kâğıdın kaç parçasından biri olduğu tartışılarak buldurulur. Çalışma yaprakları ile konu tekrar kontrol edilir. Bir kare şeklindeki bir kâğıt yüz eş parçaya bölünerek, öğrencilere renkli kalemler dağıtılarak bu karelerin belli bir bölümü taratılır, taranan bu bölgelerin alanları tartışılır. Diyagramlarda yuvarlama; kare şeklinde ve yüzer parçalara bölünmüş çalışma yaprakları öğrencilere dağıtılır ve taranmış olan bu çalışma yapraklarının alanları en yakın yüzlüğe yuvarlatılır nedenleri tekrar ettirilir. Denk kesirlerin kâğıt üzerinde taranarak parça sayısı bakımından farklı, taranan bölge bakımında alt alta bırakılarak karşılaştırılır ve denk olduğu keşfettirilir. Yüzde bulma çalışmalarında yine çalışma yaprakları dağıtılarak sorulan yüzdeliği taramaları istenir. Sonuçlar tartışılır. Düzgün taranmayan bölgelerin yaklaşık Oranları üzerinde durulur. Orantı kavramında birbirine denk iki kesir başka ne anlama gelebileceği hangi sayılarının çarpımında eşit iki sayı elde edilebileceği tartışılarak içler dışlar çarpımına hazırlık yaptırılır. Tablolar kullanılarak orantılı sayılar tablolara çizdirilir. Günlük hayatta sayılar kesirler oranlar konusunda örnekler verilerek öğrencileri kendi örneklerini oluşturmaları istenir

Birinci bölüm değerlendirilecek olursak; müfredatımıza uygun olduğu ve öğretmenlerimiz tarafından izlenirse yararlı olabileceği söylenebilir. Bölüm benzer yabancı kaynaklara göre uygulama ve çalışma yapakları ile dikkat çekmektedir.

IKINCI BÖLÜM :ÖRÜNTÜ İLIŞKILERI VE FONKSIYONLAR

Bu bölümde; tamsayı dizileri, beli bir kurala gore değişen örüntülerin öncelikle şekiller üzerinde eklemeler (kuyruklar) yaparak bu şeklin nasıl değiştigi izletilir.Çalışma yaprakları üzerinde etkinlikler düzenlenir. Çalışma yaprakları ile şekil örüntüleri iki şekilde birinci şekilde şekiller verilerek örüntünün bulunması istenir.İkinci şekilde ise örüntünün kuralı ve adım sayısı verilerek örüntünün çizilmesi izlenir.Bir çarpan olarak sıfır örüntüsü verilerek açıklanır.

4x3=

3x3=

2x3=

1x3=

0x3=

Örüntüsü çubuklar kullananılarak nasıl üçer üçer azaldıgı tatışılır ve sonuç kendi cümleleri ile ifade ettirilir. Ondalık örüntülerde yüzlük kareler dagıtılarak üzerinde örüntü oluşturmaları istenir.Paylaştırma örüntülerinde; örneğin hazır çizilmiş 6x5 birim karelerin kaç satır ve kaç sutun oldugu sorulur renkli kalemlerle istene sayıda satır veya sutunlar boyatılır ve buna bağlı bir örüntü ile konu tatıştırılır.Bir sayının bölenleri etkinliğinde çocuklara üzerinde üç tane sayı bulunan kartlar dagıtılır.Bu kartların üzerinde bulunan rakam ve sayıların hang sayının (sfir hariç) bölenleri örüntüsü oldugu sorulur. Örneğin 1,3,9 örüntüsü 27 nın pozitif bölenler oldugu gibi.

Bölen olarak sıfır örüntüsünde

Alıştırma 1	Alıştırma 2
12/4=	20/5=
12/3=	20/4=
12/2=	20/2=
12/1=	20/1=
12/0=Tahmini olarak ne olur?	20/0= tahmini olarak ne olur?

Bölmenin paylaştırma anlamını kullanarak sonucun ne olabilecegi tartışılır.

Örüntülerin karşılaştırılmasında; örüntülerin içindeki şekiller sayılar ile birebir karşılaştırılarak örüntü oluşturulur veya verilen bir örüntünün kuralı ve adım boyu buldurulur. Çalışma yaprakları ile desteklenerek konunun tartışılmasu sürdürülür.Desen oluşturma etkinlikleri ile örüntü çalışmalarına mimari bir yön verdirilir.Bölünebilem kuralları ile ilgili örüntülerde şekil ürüntülertinden yararlanarak bölünebilme kuralları kontrol edilir. Sayıların kuvvetini (üssünü) işlemlerinde örüntülerden yararlanarak açıklamak yararlı olabilmektedir. Örneğin birim kareler kullanılarak 10 veya 10n örüntü olarak gösterilmesi tartışılarak işlenmesi faydalı görülmektedir.

İkinci bölümü degerlendirecek olursak; Örüntü çeşitleri bakımından zayıf kaldıgı fakat bazı cebirsel kavramları örüntüler destegi ile işlenmesi üstün tarafını göstermektedir.En önemli özelliği her kavramın oluştırmacı yaklaşımla işlenmesi dikkat çekmektedir.

ÜÇÜNCÜ BÖLÜM: CEBİRSEL İŞLEMLERİN GELİŞTİRİLMESİ

Bu Bölümde öğrencilerin; büyük tam sayılar, kesirlerler ve ondalık sayılarla nasıl çalışacaklarına yardımcı olmak üzere düzenlenmiştir. İki veya üç basamaklı bir sayıyı bir basamaklı bir sayı ile çarpmadan başlayıp, iki veya üç basamaklı sayı ile çarpmaya kadar geniş bir şekilde çarpma konusu işlenmiştir. Örneğin renkli kalemler kullanılarak ve her basamak ayrı renkte olmak üzere 132x4 basamaklar ayrı renkte ve isimlendirilerek işlenmektedir.

Bir sayı çarkı oluşturularak çark çevrildikçe oluşabilecek büyük sayıları okumak ve tek basamaklı bir sayı ile çarparak okuma etkinliği düzenlenmiştir. İki veya üç basamaklı bir sayıyı bir basamaklı ve iki basamaklın sayı ile bölme işlemleri eşit paylaştırma kavramında başlayarak işlenmiş bolca etkinlik ve çalışma yaprakları ile testeklendigi görülmektedir.Ondalık sayılarda tablolar oluşturularak ondalık sayılarda basamak kavramı işlenmiştir. Öğrencilere çalışma yaprakları üzerinde çalışma imkanı bulunmaktadır. Kesirlerde işlemlerde; bir kesirin şekille

gösterimi ve kesirin bir tam sayı ile çarpımının anlamı ve şekil ile gösterimi işlenmektedir.Kesirlerde toplama paydasının yapısına göre ayrı ayrı çalışma yapraklı etkinlikle verilmektedir. Aynı işlemler çıkarma işleminde devam etmektedir. İki kesrin çarpımında; kesirlerin çarpımı şekil üzerinde açıklanmasına ağırlık verilmiştir.Ondalık sayılarda çarpma ve bölme işlemleri çalışma yaprakları ve etkinliklerle işlenmektedir.

Üçüncü bölümü degerlendirecek olursak; Öğrencilere tam, kesirli ve ondalık sayılarla nasıl çalışacakları konusunda işlenen konuları ve yöntemlerinin faydalı oldugu fakat Kesirlerde bölme işlemi tam sayılarda bölme işlemi kavramında örnek verilerek işlenmesi. Örnegin 30/6 demek 30 un içinde kaçtane 6 oldugunu aramak demektir.O halde ½ yi ¼ e bölünmesi demek ½ nın içinde kaçtane ¼ olduğunu aramak demektir. Bir yarımım içinde 2 tane çeyrek vardır. Kesirlerde bölme işlemi yaparken neden birinci kesir aynen ikinci kesir çarpma işlemine göre tersi alınarak çarpılması gerektiği açıklanmamıştır.Aynı şekilde iki tam sayı çarpıldığında çarpım,çarpanların herbirinde büyük iken, iki kesrinin çarpımında çarpımın neden küçüldüğü açıklanmamıştır.

DÖRDÜNCÜ BÖLÜM: GEOMETRİK VE MEKÂNSAL ANLAM

Bu bölümde; oyunlar ve basit etkinliklerle öğrencilerin geometrik şekiller ve açılarını anlamalarını sağlamak amacı ile düzenlenmiştir. Her bir etkinlikte şekilleri ele alarak ve kendi materyallerini geliştirerek veya basit oyunlar oynayarak şekiller arasında nasıl farklar olduğunu benzerlik ve denklik dahil olmak üzere öğrenirler, katı cisimlerde perspektif çalışmalarını blokları inşaa ederek yaparlar, bunları yaparken geometrik şekillerin arsındaki benzerlik ve farklıklları ve açıların nasıl ölçülebileceğini öğrenirler. İki boyutlu şekillerin kendi özellikleri ile şekiller üzerinde keserek yapıştırarak etkinliklerle işlenmektedir.Verilen bir şeklin simetrisini boyalama yöntemi ile bulma çalışmasında simetrisi alınacak şeklin bir boya ile boyanması ve kağıt katlanarak simetrisinin alınması, Bir şekli aynadaki görüntüsünün çalışılması ve açıklanması,bir seklin belli açılarda döndürülmesi ve oluşan şekillerin incelenmesi, çizgili kağıtlar üzerinde kaydırma ve döndürme çalışmalarının etkinliklerle ve çalışma yaprakları ile öğrencilere yaptırtılması çalışmaları eklenmiştir.

Açıları doğru, dar ve geniş açı olarak incelenmesinde, bir kitap duvara yaslı iken kitabın eğimi değiştirilerek durumunun incelenmesi, açıların çeşitlerine göre kontrol edilmesi,Dogruların birbirine göre durumlarını çubuklar kullanılarak tartışılması, şekillerin beli ölçülerde genişletilmesi veya küçültülmesi çalışma yaprakları üzerinde noktalı kâğıtlar üzerinde işlenmesi, Üç boyutlu nesnelerin görünen yüzlerinin veya noktalarının gözlenmesi şekil blokları ile canlı olarak gözlenmesi ,döndürülerek tartışılır.Kağı kullanarak açılar yapmak, bir açının nasıl ölçüldüğünü tartışmak, bir yarım daire ile açı ölçer yapmaya çalışmak, bir açıyı çizmek ve ölçmek, sag el veya sol el açı ölçer geliştirmek ve çalışma yapraklaı üzerinde etkinlilerin yaptırılmıştır. Açıları birleştimek ölçülerini toplamak için bir üçgenin iç açılarını keserek bir doğru üzerinde birleştirme çalışması ile üçgenin iç açıları toplamının doğru açıya karşılık geldigini yani 180 derece olduğunun görülmesi işlrnmiştir.Açı çarkı ile değişik ölçüde açıların tartışılması, çokgenlerin kenarlarına göre sınıflandırılması, iç bükey ve dış bükey çokgenlerin çizdirilmesi çalışma yaprakları ve etkinliklerle konuların kavratılması, üçgenlerin kenarlarına ve açılarına göre etkinliklerle nasıl adlandırıldığının tartışıldı , katı cisimlerin özellikleri ile birlikte şekiller üzerinde işlendiği görülmektedir. Açı ortay ve açı ortayı çizdirilmesi,açının kenarlarında dikme çıkarak dikmelerin kesiştiği noktanın açının köşesi ile birleştirerek uzatılmasında açı ortayın çizildiği görülmektedir. Sınıf içinde doğru çizme bulma çalışmalarında; sınıfta bulunan bütün nesnelerdeki (örneğin kapı,pencere,sıra,dolap.tahta.askı gibi) doğru ve doğruların birbirine göre durumları inceletilir.İçinde değişik geometrik şekiller bulunan ve bir bütün olarak dikdörtgen şeklinde birleştirilmiş tangramın sınıf içinde tanıtılarak üzerinde soruların sorulması,öğrencilere çalışma yaprakları üzerinde yaptırılması, çokgenler üzerinde pazıl (puzzling) oyunlarının oynatılması öğrencilere oyunla öğretim örnekleri olarak gösterilebilir

Dördüncü bölümü degerlendirecek olursak; konuların çalışma yapraklı ve etkinlik temelli işlenmesi, yeri geldikçe oyunlarala desteklenmesi olumlu fakat eksikliklerde vardır. Şöyleki ; Katı cisimler ve özeliklerinin işlenirken kartondan yapılan şekillerin açılması ve kapatılması ile açık seklinin nasıl oluştuğunu canlı gösterilmesi gerekir. Tangram çalışmasında hazır tangram materyalinin sınıfta öğrencilere tanıtılması ve parçalarını ayırarak her parçanın isimlendirilmesi ve özelliklerinin tekrar ettirilmesi sonrada tekrar birleştirilerek tamamlanması, öğrencilerin

benzer şekilde kartondan aynı materyali yapmaları ve üzerinde tartışmaları yararlı olacağı düşünülmektedir.

BEŞİNCİ BÖLÜM: ÖLÇME

Bu bölümde; öğrencilere ölçme kavramı içinde basit ölçmeler, yarıçap, çap, cisimlerin çevreleri, çemberin çevresi, alan ve hacim özellikle pi uygulamalı ve eğlenceli etkinliklerle anlamalarını güçlendirmek için işlendiği görülmektedir. Düzlemsel bir şeklin çevresini bulma etkinliğinde, bir bahçenin çevresini çit ile çevirme çalışmaları yaptırılır bu çalışma ile ilgili tartışma ve sorular sorulur. Bu konuda oyun etkinliği düzenlenir. Ağırlık ölçme etkinliklerinde elbise askısı kullanılarak hangisi daha ağir çalışmaları,elealınan bir cismin tahmini agırlıgının bulunması etkinliği, zaman ölçme etkinliklerinde, Bir yolun yada yapılacak bir işin ne kadar zaman alabileceği ile ilgili etkinlikler ve tahmin çalışmaları yapıldığı görülmektedir.Bir düzgün şeklin içinde kaç tane kare vardır etkinliğ ile satır ve sutun ile kısadan saydırma işlemlerinin yaptırıldığı, alan ölçme çalışmalarının çalışma yaprakları üzerinde işlendiği, dikdörtgen gibi bir alanın birim karelere bölünerek alanının o birim kare cinsinden bulunması etkinliği, dikdörtgenin alanını neden uzun kenar ve kısa kenar uzunluğunun çarpılarak bulunduğunu açıklanmıştır. Paralelkenarın alanını bulurken; makas kullanılarak paralar kenarın dikdörtgene çevrilmesi etkinliği paralelkenar alanının neden taban ile yüksekliğinin uzunlukları çarpımı olduğunu açıklaması bakımında anlamlıdır. Benzer çalışma yamuk içinde etkinlik üzerinde yapılmıştır. Şöyle ki yamuğun orta tabanı çizildikten sonra bütün yamuk birim karelere bölünür. orta tabanın üstündeki birinim kareler olduğu gibi orta tabanın altındaki birim kareye eklenir ve bir dik dörtgene dönüştüğü görülür. Bu da yamuk alanının neden orta taban ve yükseklük uzunluklarının çarpımı olduğunu açıklamaktadır. Dik prizma oluşturma etkinliğinde; ikiyüz tane A-4 kâğıtlarının üst üste konularak bir top A-4 kâğıdı oluşturularak artık üç boyutlu olduğunu ve hacminin üç boyutunun çarpımı ile bulunabileceğinin çalışma yaprakları üzerinde yaptırılması dikkat çekmektedir. Noktalı kâğıtlar kullanılarak başta üçgen olmak üzere geometrik şekillerin alanlarının etkinlik temelli işlendiği görülmektedir. Çemberin alanı birim karelere bölünerek bu biri karelerin toplanması ve boşlukların karşılıklı olarak düzeltilmesi etkinliği ile keşfettirilme çalışması yaptırıldığı görülmektedir.

Beşinci bölümü değerlendirecek olursak; Etkinlik temelli açıklamalar güzel fakat doğal ölçü birimlerinden ve standart ölçü birimlerine geçiş nasıl gelişti, ağırlık ölçü birimleri, zaman ölçme birimleri kıssaca açıklanması faydalı olurdu, alan bağıntıların işlenirken diğer alan bulma çalışmaları da yapılmalıydı örneğin eşkenar dörtgen ve deltoid eksik kaldı. Bir dairenin alanı birim dairelere bölünerek elde edilen daire dilimlerinin bir ters bir düz şekilde yan yana dizilirse,(daire dilimleri ne kadar küçük olursa) daire alanının dikdörtgenin alanına dönüştüğü ve bunun dairenin alanı neden $\pi r2$ oldugunu açıklaması daha açıklayıcı olabilirdi.

ALTINCI BÖLÜM: OLASILIK ve İSTATİSTİK

Bu bölümde olasılık ve istatistik kavramının tanıtılması amaçlanmaktadır. Hangi kesirlerin olasılık olarak kullanılabileceğini, adım adım verilerle çalışmayı ve grafiklerini çizmeyi, verilerin ortalamasını ortancasını ve tepe değerini öğrenir. Bir veri grubunu nasıl düzenleyebileceğini ve çıktılarını nasıl yorumlayabileceğini öğrenir. Bir oranın sadeleştirilmesi ve genişletilmesi etkinliği ile başlanır.Buna en güzel örnek İnka Kuş Desenleridir. Bu desende herhangi bir şeklin belli ölçüler içinde nasıl büyütülüp küçültülebileceği anlatılmaktadır.Temel mantığı verilen desenin birin karelere ayrılarak bu birim karelerin büyütüğlüp küçültülmesidir. Sayı ikililerinin anlamı üzerinde etkinlikler ve grafikleri çalışma yaprakları ile işlenmektedir.Verilerin listelenmesi ve düzenlenmesi verilerin frekasları belirlenerek grafiklerinin çizilmesi,çubuk grafikleri elle işlenerek birleştirilmesi yolu ile uygulamalı gösterilmiştir.Verilen bir durumdan istenen durumun olabilme olasılıkları çıktıları ne olabilir tartışılarak tablolarının yapılması oyunlarla konunu tekrar gözden geçirilmesi,mevcut durumda bunu nası yapabilirim? İle bir konudaki olasılıkların üzerinde düşünebilme etkinlikleri dikkat çekmektedir. Örneğin B,G,R,Y harflerini kullanarak (harfler bir defa kullanarak) kaç farklı 4 harfli kelime yazılabilir. Burada permütasyona hazırlık çalışması yapılmaktadır.Belli desenler kullanılarak kaç farklı desen oluşturulabilir ile tekrar sıralama çalışması yapılmaktadır. Çalışma yaprakları kullanılarak öğrencilere yaptıklarını uygulama fırsatı verilmektedir. Veri dizisinde Ortada Hangisi oyunu ile aritmetik

ortalamaya hazırlık, Ortanca Avcısı ile ortanca kavramına hazırlık yapılmaktadır. Çalışma yaprakları ile Medyan avcısı ve Medyan çarkı etkinlikleri yapılmaktadır. Basit bir olayda mümkün olan yolları karşılaştırması üzerinde tartışma, olasılık çalışma yaprakları ile olasılığın derinlemesine anlaşılması sağlanmaktadır. Kavramların örnekler üzerinde uygulamalı açıklanması dikkat çekmektedir.

Altıncı bölümü değerlendirecek olursak; Bir alıştırma kitabı olarak hazırlanan kitabın, öğrenci yaşına ve seviyesine göre özenle hazırlandığı söylenebilir fakat bazı temel kavramları tanımlanması faydalı olabilirdi.

YEDİNCİ BÖLÜM: SAYI TEORİSİ

Bu bölümde amaç temel sayı kavramlarını öğrenilmesine yardımcı olmaktır. Bunlar tek sayı ile çift sayı arasındaki fark, ortak payda alma kavramı, Ortak Katların En Küçüğü, Ortak Bölenlerin En Büyüğü, faktöriyel kavramı, asal sayılar konularının etkinliklerle, oyunlarla işleyebilmektir.

Bir tam sayının tek veya çift olduğunu belirleme etkinliği, satırların bileştirilmesi etkinliği, satır sütün sayılarının çarpımında oluşan sayıların anlamı, Sayı oluşturma etkinlikleri örneğin verilen iki kümeden belli kurallar içinde her kümeden bir sayı alarak yeni sayılar oluşturmak etkinliği ile sayı işlemleri konusunda yeteneklerini geliştirmek istendiği görülmektedir. Sayı oluşturmak için desenler, çarpanların renklendirilmesi etkinliği ile bir sayının çarpanlarının nasıl bir dizi halinde değiştiğini bir örüntü oluşturduğunu renkli kalemler kullanılarak işlenmektedir. İki veya daha çok kesir in en küçük ortak paydasını (Paydalarını eşitlemek) bulma etkinliğinde kutularla çalışarak paydalarını eşitlemek, denk kesirleri kutuları kullanarak bulma etkinliği örneğin bir bütün iki eş parçaya bölünmesi ½ ile, Aynı bütünün dört eş parçaya bölünmesi ve iki parçasının alınması da 2/4 ile gösterilmesine rağmen bu iki kesir aynı bölgeyi göstermektedir. Dolayısı ile denktir. Payda bulma çarkı ile çalışma yaprakları üzerinde işlenmekte olduğu görülmektedir. Tam sayıları asal çarpanları bulma etkinliğinde matris kutularında yararlanarak asal çarpanlarını bulma çalışması dikkat çekmektedir. Bir tam sayını çarpan ikililerini bulmak için sayını asal çarpanlarını

kullanmak Örneğin 30; 2x(3x5).bütün etkinlikler çalışma yaprakları ile desteklenmiştir.

Yedinci bölümü degerlendirecek olursak; Sayı teorisi çok geniş bir konu olup, bu konunun temelini böyle basit ve etkili işlenmesi dikkat çekmektedir.Özellikle çalışma yayrakları derse farklı bir anlama çeşitliliği kazandırdıgı söylenebilir.Burada tanımların bilindigi kabul edilerek etkinliklerin düzenlendiği görülmektedir.Kısa hatırlatıcı tanımlamalar yapılabilirdi.

SEKİZİNCİ BÖLÜM: CEBİRSEL DÜŞÜNME

Bu bölümde; öğrencilere cebirsel düşünme tanıtılır.Eğlenceli etkinlikler ve oyunlarla öğrenciler cebirsel bir ifadeyi yazmayı öğrenir.Pozitif ve negatif tam sayılarla işlem yapmanın farkına varır. Basit cebirsel denklemlerin çözümüne ek olarak üç temel cebirsel teknikleri ve nasıl kullanılacağını öğrenir.

Bir hikaye ile cebirsel ifade ve yansımaları işlenir. Cebirsel ifadede bilinmeyenin canlandırılması etkinliği, cebirsel ifadelerde yer değiştirme işlemleri etkinliği, pozitif ve negatif sayının cebirsel ifadedeki anlamı ve işlem sırası, tamsayıları gösterimi etkinliği, cebirsel ifadelerde gruplandırma çalışmaları ,tamsayılarda dört işlem etkinlikleri, cebirsel ifadelerde denge ve denklemlerin çözümündeki önemi, Bir cebirsel ifadede yer değiştirme çalışmaları,yerine yazma etkinlikleri, ekleme ve çıkarma etkinlikleri, bilinmeyeni dengelemek, denklem zorlukları etkinliği, yapılacak hareketi tahmin etme etkinlikleri, çalışma yaprakları üzerinde işlenmesi olumlu değerlendirilmektedir.

SONUÇ

Bir kitap incelemesi olarak ele aldıgımız bu çalışmadan; Kitabın tamamında yapılandırmacı öğrenme yaklaşımı kullanıldığı bu konuda çok az kitap bulunduğundan bu hususun degerl,i olduğu söylenebilir. Kitabın

kapsamı ve elealınış işleniş biçimi olarak bir ders kitabı değil bir yardımcı kaynak olarak kulanılabilecegi, bir yardımcı kaynak olarak etkinliklerin uzun zaman alabileceği düşünülerek öğretmenlerin bu kaynağı incelemelerinde fayda olabileceği ve istedikleri uniteleri seçerek kullanabileceklerini. Her bölümün sonunda yapılan değerlendirmede belirtildiği gibi eksikleri olmasına rağmen bir uygulama kitabı olarak eğitimcilerin elinde bulunması gereken bir kitap olarak değerlendirilebilir.Yabancı dille yazılmasına rağmen basıt bir anlatım yolu tercih edildiği görülmektedir.Bu yönü ile akademisyenlere bu güzel uygulama kitabının çevrisinin yaparak literatüre kazandırma konusunda fırsat sunmaktadır.

KAYNAKLAR

Thompson,M.,F"Hands On MATH READY TO USE GAMES &ACTİVİTİES FOR GRADES (4-8)" The Center For Applıed Research In Educatıon,U.S.A, ISBN: 0-87628-383-0 (S) , ISBN:0-8728-388-1 (P)

BÖLÜM2

2. KATMAN İÇ AĞ SALDIRILARI ve ÖNLEMLER

YL. Öğrencisi Hanifi TOPRAK
Dr. Öğr.ÜyesiSüleyman KARDAŞ

2. KATMAN İÇ AĞ SALDIRILARI ve ÖNLEMLER

LAYER 2 INTERNAL NETWORK ATTACKS AND THE COUNTERMEASURES

Hanifi TOPRAK
Yüksek Lisans Öğrencisi, Batman Üniversitesi Fen Bilimleri Enstitüsü, Elektrik Elektronik Mühendisliği Anabilim Dalı, (Sorumlu Yazar)

Süleyman KARDAŞ
Dr. Öğr. Üyesi, Batman Üniversitesi Mühendislik ve Mimarlık Fakültesi,Bilgisayar Mühendisliği Bölümü,

1. GİRİŞ

Her geçen gün hızla gelişen bilişim teknolojileri insanların da internet kullanıcısı olmayı zorunluluk haline getirmiştir. Dünya nüfusunun %56'sı (4.38 Milyar) internet kullanıcısıdır [1]. İnternetin kullanımında bu denli bir artışın olması kolaylık ve özgürlük gibi faydalarının yanında kişileri ve sistemleri hedef haline getirmesi gibi dezavantajları da mevcuttur. Dünyanın yarısı bazı insanlar için hedef durumundadır. Siber saldırı, hedef sistemlerin erişilebilirlik, bütünlük veya gizliliğine karşı yapılan, kişi veya kişiler tarafından yapılan işlemdir. [2]. Toplam siber saldırılar her geçen gün artmaktadır. Fakat bazı saldırı türlerinde de düşüşler meydana gelmektedir. Bulaştığı sistemlerin dosyalarını kriptolayıp bunun şifrelerinin çözülmesi için ücret isteyen Ransomware (Fidye) yazılımlarında 2015 yılı içerisinde 3.8 milyon, 2016 yılı içerisinde 538 milyon ve 2017 yılı içerisinde 183.6 milyon saldırı Sonicwall tarafından tespit edilmiştir [3]. 2016 yılından bu kadar yüksek iken 2017 yılında düşmesinin nedeni bu saldırı çeşidine karşı geliştirilen önlemler olmuştur. Bunu gören saldırganlar farklı saldırı türlerine yönelmiştir. Siber saldırılar kurum bilgi varlıkları için hayati bir öneme sahiptir [4]. Kurumsal

yapılarda kurum dışından yapılacak siber saldırıların önlenmesi için güvenlik duvarları ve SIEM (Security Information and Event Management – Bilgi güvenliği Tehdit ve Olay Yönetimi) yazılımlar üzerinde gerekli yapılandırmalar yapılarak sistemler korunaklı hale getirilmesi mümkündür. Fakat 2. Katman Saldırıların güvenlik duvarı ya da atak tespiti yazılımları tarafından tespiti mümkün olmamaktadır. Çünkü bu saldırılar Local Area Networklerden yapılmaktadır. Üniversitemiz örneğine baktığımızda vlan'lar omurgada sonlandığından bunları tespit etme şansımız bulunmamaktadır. Bir ağın güvenliği tam anlamıyla sağlayabilmek için dışardan yapılacak (WAN) saldırıların yanında içerden (LAN) de gelebilecek saldırıların tespitinin yapılması ve gerekli önlemlerin alınması gerekmektedir. Bu çalışmada öncelikle siber güvenlik ve iç ağda yapılan katman 2 saldırıları hakkında bilgi verilecek ve bu saldırılara karşı alınabilecek önlemler sunulacaktır.

2. BÖLÜM SİBER GÜVENLİK

2.1 Siber Tanımı

Siber kelimesi "sibernetik" kökünden gelmektedir. Sibernetik ise kendi kendine denge kurarak kontrol etme ve yönetme anlamındadır. İnsan yaşamı ile makinelerin yönetişimi şeklinde birbirleri ile bilgi alış-verişi olarak "Siber" terimi tanımlanabilir [5]. Günümüzde ise daha çok sanal erişim veya sanal yaşam olarak kullanılmaktadır.

2.2 Siber Güvelik

Siber saldırılara karşı alınacak topyekûn önlemlerdir. Saldırganlar, hedef sistem, kurum ya da kişiye çeşitli yöntemlerle saldırı gerçekleştirmektedir. Siber saldırganlar sistemlerin normal iş süreçlerini kesmek ya da yavaşlatmak isterler [6]. Siber saldırılardan korunmak için Başarılı bir siber güvenlik yaklaşımına ihtiyaç vardır. Bu yaklaşımda birden fazla katman bulunmaktadır. Bir kurum veya kuruluşta, bir bütün olarak saldırılara karşı önlemler alınabilir. Çalışanlar ve teknolojik alt yapı birbirini tamamlamalıdır [6].

2.3 Siber Saldırı

Hedef sistem üzerinde saldıran kişi veya kişilerin amaçlarını elde etme için yapılan girişime verilen addır. Hedef sistemin çalışmasını durdurma ya da hedef sistemden veri çalma gibi amaçlar güdülebilir.

2.4 USOM

20 Haziran 2013 Yılında ülkemize yönelik yapılmış siber saldırıların tespit edilmesi, yapılacak olanların bertaraf edilmesi ve etkilerinin azaltılmasına yönelik Bilgi Teknolojileri ve İletişim Kurumu altında Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) kurulmuştur [7]. USOM, Uluslararası ve ülke içinde sanal ortamda öngörülen tehditlerle ilgili kendisine ulaşan bildirimleri yorumlar ve boşa çıkarmak için Kamu Kurumları ve Özel Sektörle iletişim halinde olur. Bu bağlamda kendisine ulaşan bildirim ile ilgili çözümleme ve sonuçlandırma işlemini yürütür ve takipçisi olur [7]. Aynı zamanda yurt içi ve yurt dışı tatbikatlar yaparak yurttaki siber saldırılara yönelik farkındalık yaratır.

2.5 Kurumsal SOME

Siber Olaylara Müdahale Ekibinin kısaltılmış halidir. Kurumlarına yapılan veya yapılması planlanan siber saldırılara yönelik önlem alma, gerektiğinde USOM ile iletişime geçmekle yükümlüdürler. Kurumsal SOME'ler, Kurumların teknik alt yapı ve idari kısımlarında siber güvenlik konusundan önerilerde bulunurlar. Kurumsal SOME; Bakanlıklar, Müstakil Kamu kurumları ve Bilgi İşleme sahip kamu kurumlarından oluşmaktadır. USOM tarafından verilen görevleri yapmakla mükelleftir [8].

3.BÖLÜM OSI Referans Modeli ve 2. Katman (Layer 2) saldırıları

3.1 OSI (Open System Interconnection)

ISO aynı networkteki cihazların birbirleri ile olan iletişimi nasıl olacağı ile ilgili kuralları OSI modelinde tanımlamaktadır. 1984 senesinde OSI referans modeli olarak yayınlanmıştır. OSI referans modeli öncesi aynı networkteki cihazların haberleşmesi mümkün olmamaktaydı. Bu nedenle tüm cihazlar aynı üreticinin cihazı olmak durumundaydı. OSI referans modeli sayesinde bu dezavantaj ortadan kaldırılmış oldu. OSI referans modeli 7 katmana ayrılmaktadır.

Bunlar aşağıdaki gibidir.

1. Fiziksel Katman
2. Veri Bağlantı Katmanı
3. Ağ Katmanı
4. Taşıma Katmanı
5. Oturum Katmanı
6. Sunu Katmanı

7. Uygulama Katmanı

3.1.1 Fiziksel Katman

Fiziksel katman verinin kablo üzerinde alacağı yapıyı tanımlar [9]. Bu katmanda veriler bit olarak iletilir. Bu katman 1 ve o'ların nasıl ışık, elektrik veya radyo sinyallerine çevrileceğini ve aktarılacağını tanımlar. Veri bu katmanda göndericide 1ve 0'lar elektrik sinyaline dönüştürülüp kabloya yerleştirilir, karşı tarafta da bu elektrik sinyalleri okunu ve 0 ve 1'lere dönüştürülür. Verinin karşı tarafa, kullanılan fiber optik kablo, bakır kablo, radyo sinyalleri üzerinden nasıl gönderileceğini Fiziksel katman tanımlar. Veri akışının mümkün olabilmesi için iki tarafın aynı kurallar üzerinde tanımlanmış olması gerekir. Fiziksel katmanda bulunan cihazlara kablo, fiber optik, hub ve tekrarlayıcı örnek verilebilir.

3.1.2 Veri Bağlantı Katmanı

Veri bağlantı katmanı fiziksel katman ile ağ katmanı arasında bağlantıyı sağlamaktadır. Fiziksel katmandan alınan bitleri ve ağ katmanında almış olduğu veri paketlerini framelere dönüştürür. Veri bağlantı katmanının büyük bir bölümü Ethernet kartı içinde gerçekleşir. Veri bağlantı katmanı ağ üzerindeki diğer bilgisayarları tanımlama, kablonun o anda kimin tarafından kullanıldığının tespiti ve fiziksel katmandan gelen verinin hatalara karşı kontrolü görevini yerine getirir [9]. İkinci katman cihazlara modem, network kartı ve switch (anahtar) örnek verilebilir.

3.1.3 Ağ Katmanı

Verinin başka bir ağa iletilmesi durumunda yönlendiricinin kullanacağı bilgi Ağ katmanında eklenir. Bağlantı katmanındaki çerçeveler bu katmanda paketler dönüştürülür. Ağ katmanında gönderen ile alıcı arasında en uygun yoldan verinin taşınması kontrol edilir. Bu katman sayesinde verinin yönlendiriciler (router) aracılığıyla yönlendirilmesi sağlanır. IP, IPsec, CLNS bu katmanda çalışır.

3.1.4 Taşıma Katmanı

Taşıma katmanı verinin küçük paketlere bölünüp (Karşı tarafın alabileceği kadar büyüklükte) gönderilmesinden sorumludur. Karşı taraftan gelen iletildi mesajından sonra sonraki paketin gönderilmesi

işlemine geçilir. Bu katmanda veriler frameden segmente dönüşür. Bu katmanda çalışan protokollere TCP, UDP örnek verilebilir. Taşıma katmanı aynı zamanda verinin hatasız bir şekilde iletilmesinden de sorumludur. TCP bağlantısında veri çarpışmalardan dolayı karşı tarafa doğru iletilmemiş ise tekrar gönderilir. UDP bağlantıda ise tekrar gönderme işlemi yapılmaz [10].

3.1.5 Oturum Katmanı

Oturum katmanında birden fazla cihaz ile iletişim halinde olunması durumunda gerekli ayarlamaları yapar. Oturum ile bağlantı arasındaki koordinasyonu sağlar. Bir cihazın en az iki bilgisayarlarla aynı anda haberleşmesi durumunda, doğru cihaz ile iletişimini sağlar. Sunuş katmanına yollanacak veriler farklı oturumlarla birbirinden ayrılarak yapılır. Bu katmandaki protokollere NetBIOS ve Sockets örnek verilebilir.

3.1.6 Sunuş Katmanı

Bu katmanın en önemli görevi yollanan verinin karşı cihaz tarafından anlaşılacak şekilde çevrilmesidir. Bu sayede farklı programların birbirlerinin verisini kullanabilmesi mümkün olur. Sunum katmanı, verinin kaynağında formatının belirlenmesi ve bunun karşı tarafta anlaşılmasından sorumludur. Veri bu katmanda şifreleme ve şifre çözmeler yapılır. Mov, JPEG vb. bu katmanda çalışır.

3.1.7 Uygulama Katmanı

Uygulama katmanı kullanıcılara en yakın olan katmandır. Kullanıcılar çeşitli yazılımlar sayesinde (web tarayıcısında işlem yapmak gibi) verilerini oluştururlar. OSI katmanlarında sadece bu katman diğer katmanlara servis sağlamaz. Uygulamaların ağ üzerinde çalışması sağlanır. Bu katman kullanıcıların gereksinimini karşılar. DHCP, SSH, FTP, SNMP, HTTP, DNS protokolleri ve tarayıcılar bu katmanda çalışır.

3.2 MAC Adres Taşması

MAC Adres Taşması en çok yapılan 2. Katman saldırısıdır. Bu saldırı türünde saldırgan anahtarlayıcıya (Switche) çok fazla sahte MAC Adresi gönderir. Art arda gelen mac adresleri switchin mac adres tablosunu

doldurur ve yeni gelen cihazın mac adresi, mac adres tablosuna kaydedilmeyecek duruma gelir. Norma şartlar altında gelen çerçevelerin içerisinde hedef cihazın mac adresi bulunur fakat eğer switchte belirtilen mac adresi bulunmuyorsa veri o switche bağlı tüm portlara gönderilir. Bu durumda saldırgan gelen paketi alır ve dinleme yapabilir. Bu saldırıda paketler tüm portlara iletildiğinden o switch üzerinde gereksiz bir trafik de söz konusu olur. Bu saldırıya aşağıdaki yöntemler ile önlem alınabilir.

3.2.1 Port Security

Switchin her portunda gelebilecek mac adresi limiti belirlenir. Bu durumda saldırgan mac adresi gönderse bile mac tablosuna kaydedilmeyecektir. Bu yöntemin dezavantajı ilgili porta başka gerçek bir cihaz takılması durumda da networke dahil olamayacaktır.

3.2.2 Authentication with AAA server (802.1.x)

Gelen mac adresi kaydedilmeden önce bir doğrulamadan geçer doğrulama yapılmayan Mac kaydedilmeyeceğinden Mac tablosuna eklenmeyecektir.

3.3 VLAN Hopping Atakları

Vlan (Sanal yerel alan ağı) aynı ağda bulunan kullanıcı veya cihazların mantıksal olarak gruplandırılmasıdır. Aynı grup içerisinde bulunan cihazlar veya kullanıcılar birbirlerine erişebilirken farklı gruplarda bulunanlar erişim şansı bulunmamaktadır. Vlan Hopping grubu dışındaki VLAN'e ulaşabilmenin sağlandığı bir saldırı türüdür. VLAN Hopping saldırısında saldırgan tüm vlanlara erişim sağlayabilmektedir. Alınabilecek önlemler aşağıdaki gibidir.

- Anahtarlama cihazının tüm portları Access moda alınır ve sadece uplink portları trunk moda çekilir.
- Trunk mode da kullanılacak portlar dışındaki portların devre dışı bırakılması gerekmektedir.
- DTP devre dışı bırakılması gerekmektedir.
- Diğer üreticilerin cihazları ile iletişim sağlanmayacaksa VLAN 1 ‘i kullanmamak.

3.4 Spanning-Tree Protokolü (STP) Atakları

Kurumsal ağlarda sık sık karşılaşılan sorunlardan bir tanesi switchlerde kullanıcılardan dolayı yapılan döngülerdir. Switch döngüleri oluştuğunda networkte yavaşlama ve kesintiler oluşmaktadır. STP sonsuz döngüleri engellemek için kullanılan protokoldür. STP’de her anahtarın(switch) bridge ID değeri vardır. Bu da “bridge priority” ve mac adresinden oluşmaktadır. “bridge priority” değeri varsayılan olarak 32768’tir.

STP'de "bridge priority" en düşük olan kök switch olur. Saldırgan ağa yeni bir switch dahil eder ve "bridge priority" değeri olarak 0 verir ve kendi konumlandırdığı switchi root switch olarak tanımlanmasını sağlar.

Bu saldırıdan korunmak için aşağıdaki yöntemlere başvurulabilir:

- Root Guard
- BPDU Guard

3.5 Sahte MAC Atağı

Saldırgan öncelikle hedef cihazın mac adresini öğrenir. Daha sonra switche gönderilen çerçevelerin içerisine hedef cihazın mac adresi yazılır. Bu durumda switchin mac adres tablosunda aynı mac adresinden (saldırılan cihaz) iki tane kayıt yer almış olur. Switche gelen paketler hem saldırgana hem de hedef cihazın portuna iletilir. Bu işlem hedef cihazın ağa paket göndermesine kadar devam eder. Trafik saldırgana da gittiği için saldırgan tarafından dinlenebilmektedir. Bu saldırıdan korunmak için aşağıdaki yöntemlere başvurulabilir:

- Port Security
- 802.1x

3.6 Sahte ARP (ARP Spoofing, ARP Poisoning) Atağı

ARP protokolü, MAC adreslerinin IP adresleriyle eşleşmesini sağlayan protokoldür. Bir cihaz haberleşmek istediği cihazın IP adresini biliyor ve MAC adresini bilmiyorsa ARP tablosuna (MAC-IP adreslerinin tutulduğu tablo) bakar. Kendi ARP tablosunda bulunmayan bir cihaz ile iletişim kurulması durumunda ise switchdeki tüm portlara ARP isteği gönderilir ve bu isteğe sadece hedef cihaz cevap verir. Paketi gönderen cihaz dönen Mac adresi ARP tablosuna ekler. Sahte ARP saldırısında, saldırgan ARP isteğine muhatap olmadığı halde cevap verir ve hedef cihazın ARP tablosuna kendi MAC adresini kaydettirir.

PC 1	10.5.10.20	f8:63:3f:43:6f:a2
Saldırgan	10.5.10.30	a8:63:3a:33:42:62
Gateway	10.5.10.254	b4:44:4b:55:22:df

Yukarıdaki topolojide PC 1 in ARP tablosunda Gateway cihazının mac adresi bulunmaması durumunda, switche ARP request isteği gönderilir. Bu isteğe Gateway cevap vermesi gerekirken Saldırgan cevap verir ve PC 1 ARP tablosunu buna göre güncelleştirir. Bu durumda PC 1 in göndereceği tüm paketler saldırgan üzerinde geçecektir. Bu saldırı Man In

the Middle (Ortadaki adam) saldırısı olarak tanımlanır. Bu saldırıdan korunmak için aşağıdaki yönteme başvurulabilir:

- Statik ARP kayıtları oluşturmak

3.7 DHCP Açlık Atağı

DHCP, ağa bağlanan cihazlara IP adresi, DNS adresi, varsayılan ağ geçidi gibi ayarları dinamik olarak iletmekten sorumlu protokoldür. DHCP Açlık saldırısında, saldırgan DHCP sunucusuna art arda DHCP istekleri gönderir ve bağlı bulunduğu scopedaki tüm IP adreslerini tüketir. Daha sonra Kendi DHCP sunucusunu ağa dahil eder. Yeni oluşan durumda ağa bağlanan cihazlar saldırganın konumlandırdığı DHCP sunucusundan IP Adresi, varsayılan ağ geçidi ve dns sunucu bilgisini alır. Saldırgan varsayılan ağ geçidi ve dns adres bilgisi olarak kendi IP adresini verir. Böylelikle tüm trafiğin kendi üzerinde çıkmasını sağlamış olur. Bu saldırı ortadaki adam saldırısı (Man In the Middle Attack) olarak tanımlanır.

Bu saldırıya karşı alınabilecek önlemler aşağıdaki gibidir:

1. 802.1x Authentication,
2. Port Security
3. DHCP Snooping
4. IP Source Guard

3.8 LAN Storm (Fırtınası)

Switchlerde bazı protokoller (DHCP, ARP vb.) broadcast yayını kullanır. Bundan dolayı switchler broadcast yayını engellenmemesi gerekmektedir. Bu durumu bilen saldırganlar ağı zehirleyecek şekilde yayın yaparlar. Buna LAN fırtınası denilmektedir. Bu saldırgan korunmak için ilgili LAN takip edilmeli belli bir eşik değeri tanımlanmalı ve bu eşik değer geçilmesi durumunda broadcast yayını engellenmelidir.

4. MATERYAL VE YÖNTEM

Test ortamı için öncelikle sanallaştırma yazılımı olan Vmware Workstation kurulumu gerçekleştirilmiştir. Daha sonra bir adet Microsoft Windows 10 İşletim sistemine sahip sanal bilgisayar kurulumu yapılmıştır. Ayrıca dünya standartlarında bilgi güvenliği eğitimi ve penetrasyon testi hizmetleri sağlayan açık kaynak kodlu Kali Linux saldırı amaçlı kurulumu yapılmıştır. Söz konusu cihazlar aynı kenar anahtarlama

üzerinde bağlantı sağlanmıştır. Kurumsal ağ örneğimizde kullanılan kenar anahtarlama HP 2610 dur.

a. Birinci aşamada normal kullanıcı iç ağa dahil olduğunda olan işlemler hakkında bilgi verilmiştir. Daha sonra saldırı esnasında ve sonrasında oluşan ağ trafiğinde paket analizleri yapılmıştır.
b. İkinci durumda ise yapılan saldırılara göre saldırı önleme işlemleri yapılmıştır. Gerekli önlemler alındıktan sonra test amaçlı birinci aşamada yapılan işlemler tekrarlanmıştır.

Ağdaki yapılan trafiğin analizleri için açık kaynak kodlu Wireshark yazılımı kullanılmıştır.

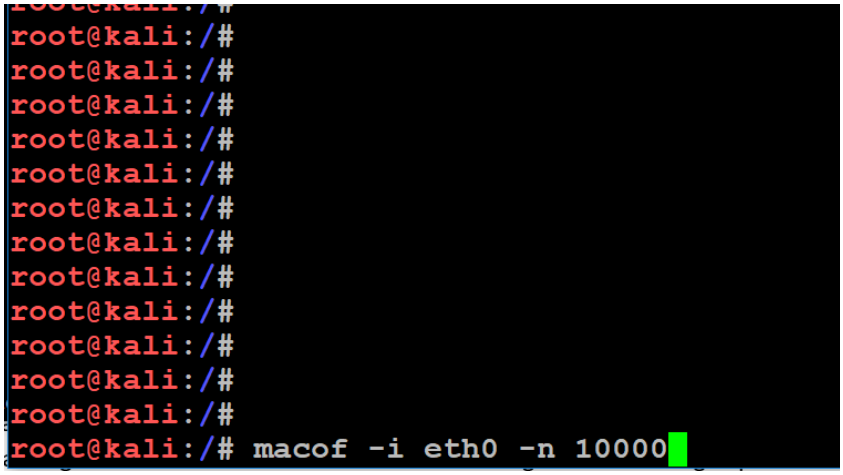
5.ARAŞTIRMA VE BULGULAR

5.1 Mac Adres Taşması Uygulaması

Bu saldırı için Kali Linux te bulunan macof aracı kullanılacaktır. Macof Aracının genel kullanımı aşağıdaki gibidir:

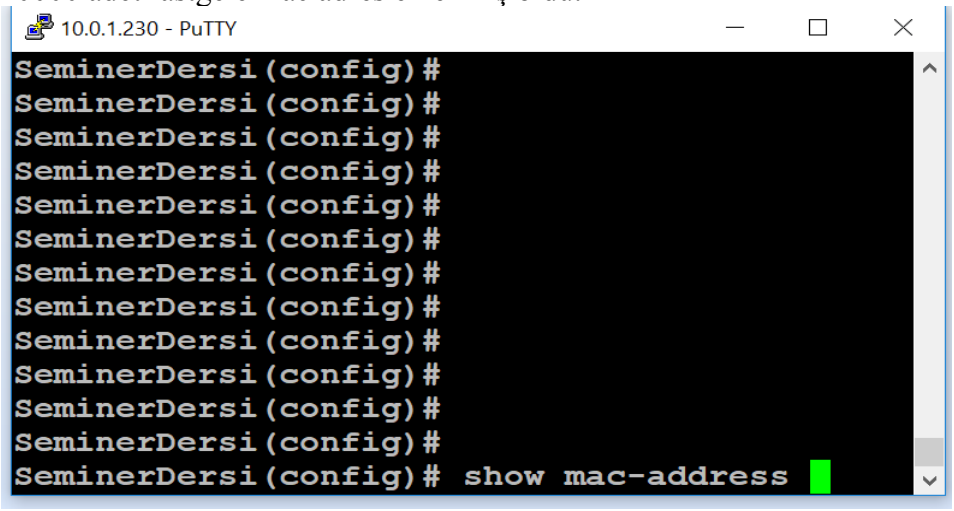
macof [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]
-i Kullanılacak Ağ Kartı
-s Kaynak IP Adresi.
-d Hedef IP Adresi.
-e Hedef Donanım Adresi.
-x TCP Kaynak Portu.
-y TCP Hedef Portu.
-n Gönderilecek Paket Sayısı.
macof -i eth1 -n 10

Yukarıdaki kullanımda, bağlı bulunan switche rastgele mac adresi gönderilir, hedef switchin Mac Adres Tablosunun dolmasına ve yeni gelen mac adresinin belirtilen tabloya kaydedilmesinin engeller. Dolayısı ile switche gelen çerçevenin hedef mac adresine bakıldığında Mac adres Tablosunda bulunmadığında Switch ilgili paketleri tüm portlara iletilmesine neden olur. Bu durumda diğer portlarda dinleme yapanlar kendisine gelmemesi gereken trafiği de dinlemiş olur.



Şekil 1. Macof Kullanımı

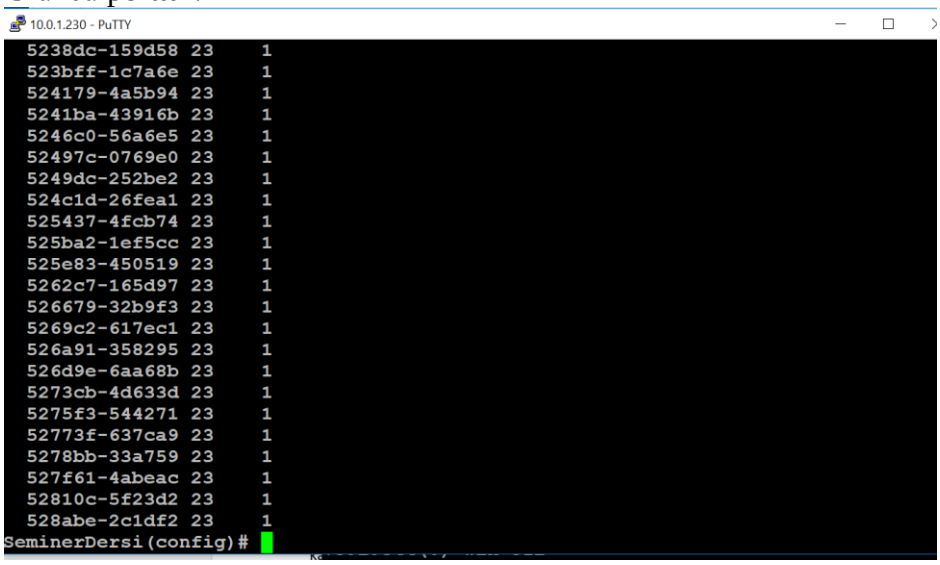
Switchinlerin mac adres tablo kapasiteleri farklı olabilmektedir. Bundan dolayı yukardaki komut ile bağlı bulunan switchin mac adres tablosuna 10000 adet rastgele mac adres eklenmiş oldu.



Şekil 2. Show Mac-Adress Kullanımı

Show mac-adress ile mac adresinde bulunan mac adresleri ve hangi porttan geldiği bilgisini gösterir (HP switchler için geçerlidir.)

Bu komutu yazdığımızda aşağıdaki gibi rastgele üretilmiş mac adresleri karşımıza çıkmaktadır. Kali Linux cihazının bağlı bulunduğu port 23'üncü porttur.

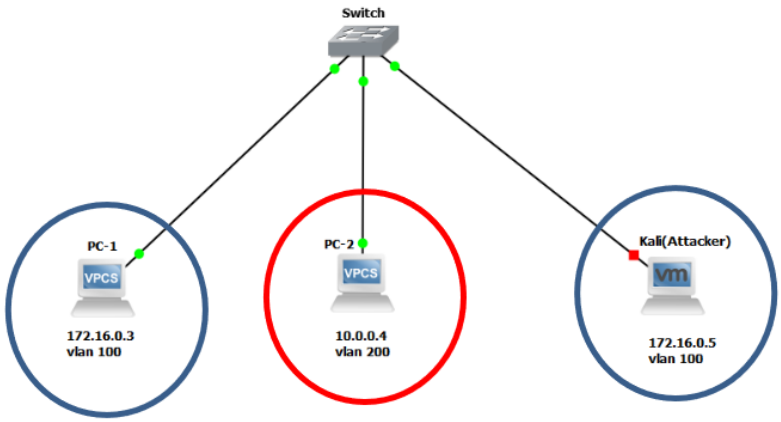


Şekil 3. Macof Sonrası Mac Adres Tablosu

Bu işlemlerden sonra mac adress tablosundan bulunmayan bir cihazın ağa dahil olması durumunda yaptığı trafiğin dinlenebilmektedir.

5.2 Vlan Hopping Uygulaması

Vlan Hopping İçin Kali Linux de bulunan Yersinia aracı kullanılacaktır. Yapımız aşağıdaki gibidir.



Şekil 4. Vlan Hopping Saldırısı Genel Topoloji

Yapıdaki PC ve saldırganın IP adresi ve Vlan ID'leri aşağıdaki gibidir.

Ad	IP Adresi	Vlan ID
PC-1	172.16.0.3	100
PC-2	10.0.0.4	200
Saldırgan(Kali)	172.16.0.5	100

Saldırgan ve PC-1 aynı vlanda olduklarından birbirlerine erişim sağlayabilmekteler.

```
PC-1> ping 172.16.0.5
84 bytes from 172.16.0.5 icmp_seq=1 ttl=64 time=38.000 ms
84 bytes from 172.16.0.5 icmp_seq=2 ttl=64 time=6.999 ms
84 bytes from 172.16.0.5 icmp_seq=3 ttl=64 time=20.977 ms
84 bytes from 172.16.0.5 icmp_seq=4 ttl=64 time=82.977 ms
84 bytes from 172.16.0.5 icmp_seq=5 ttl=64 time=14.794 ms
```

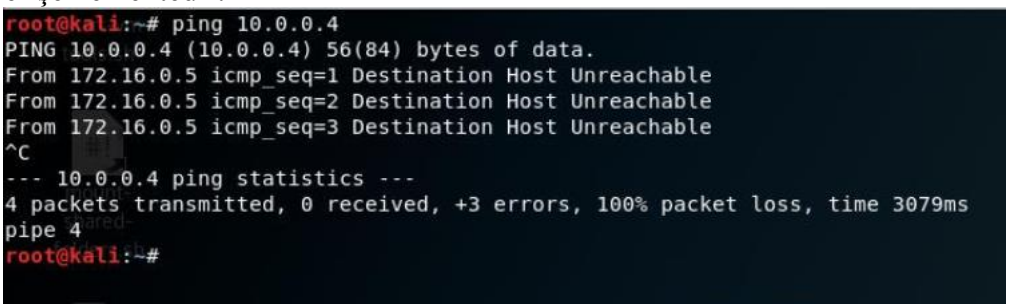
Şekil 5. Aynı Vlanda Bulunan Saldırgan Tarafından PC-1'e Yapılan Ping Sonucu

Aynı şekilde saldırgan (Kali) da PC-1 makinesine erişebilmektedir.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.0.5  netmask 255.255.255.0  broadcast 172.16.0.255
        ether 00:0c:29:3f:e4:fa  txqueuelen 1000  (Ethernet)
        RX packets 30  bytes 7545 (7.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 108  bytes 19048 (18.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2176  bytes 175920 (171.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2176  bytes 175920 (171.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# ping 172.16.0.3
PING 172.16.0.3 (172.16.0.3) 56(84) bytes of data.
64 bytes from 172.16.0.3: icmp_seq=1 ttl=64 time=37.9 ms
64 bytes from 172.16.0.3: icmp_seq=2 ttl=64 time=22.6 ms
64 bytes from 172.16.0.3: icmp_seq=3 ttl=64 time=26.0 ms
64 bytes from 172.16.0.3: icmp_seq=4 ttl=64 time=18.3 ms
^C
--- 172.16.0.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 18.387/26.263/37.967/7.283 ms
```

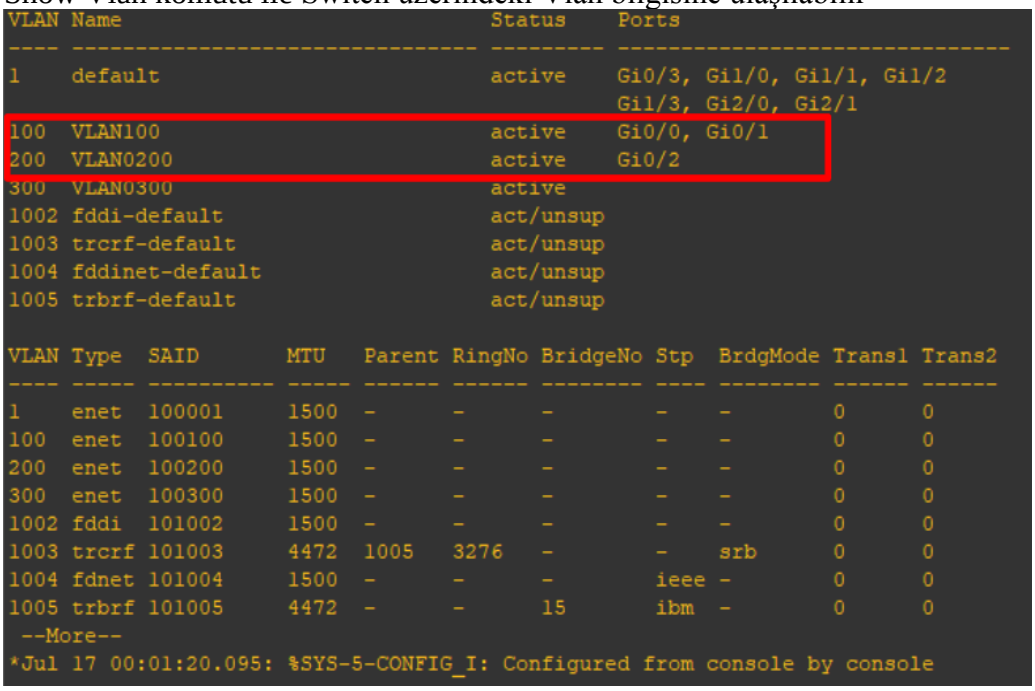
Şekil 6. Saldırgan Tarafından PC-1'e Yapılan Ping Sonucu

Fakat saldırgan (Kali) PC-2 makinesine farklı vlanlarda olduklarından erişememektedir.



Şekil 7. Saldırgan Tarafından Farklı Vlanda Bulunan PC-2'e Yapılan Ping Sonucu

Show Vlan komutu ile Switch üzerindeki Vlan bilgisine ulaşılabilir



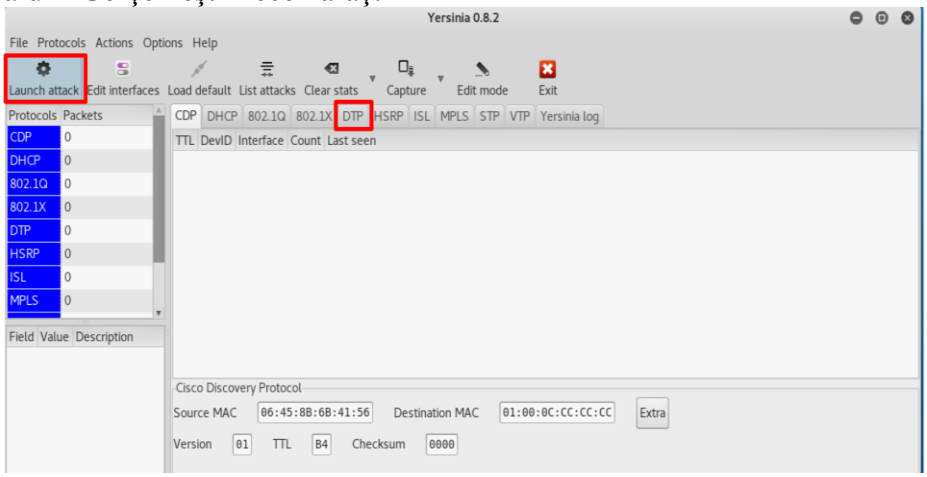
Şekil 8. Switch Üzerinde Bulunan Vlanların Listesi

Show interfaces status ile bağlı olan portların hangi vlanda olduğu bilgisine ulaşılır

```
Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/0                        connected    100          auto   auto unknown
Gi0/1                        connected    100          auto   auto unknown
Gi0/2                        connected    200          auto   auto unknown
Gi0/3                        connected    1            auto   auto unknown
Gi1/0                        connected    1            auto   auto unknown
Gi1/1                        connected    1            auto   auto unknown
Gi1/2                        connected    1            auto   auto unknown
Gi1/3                        connected    1            auto   auto unknown
Gi2/0                        connected    1            auto   auto unknown
Gi2/1                        connected    1            auto   auto unknown
```

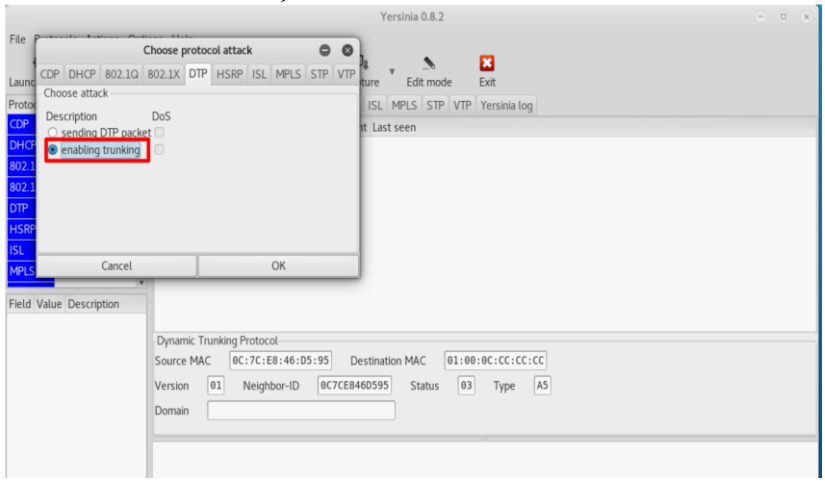
Şekil 9 Switche Bağlı Portların Bulundukları Vlanların Gösterimi

Saldırı Gerçekleştirilecek araç:



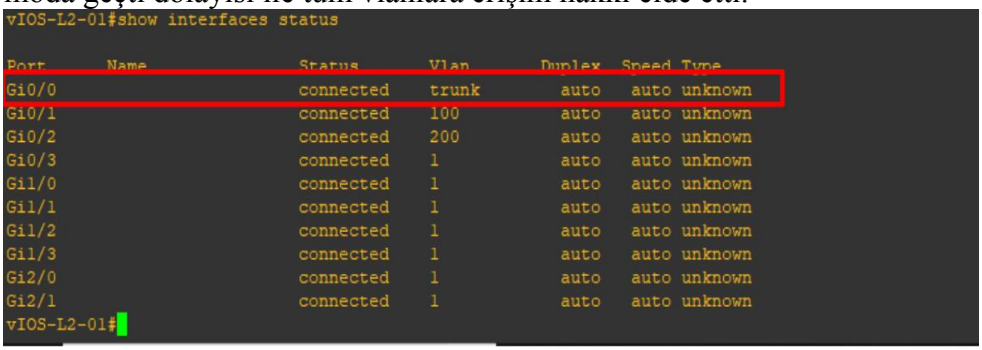
Şekil 10. Vlan Hopping Saldırısında Kullanılacak Yersinia Toolu

Yersinia Toolunda DTP seçilir.



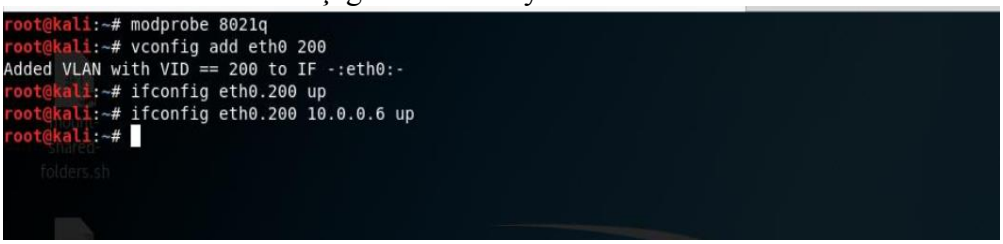
Şekil 11. Yersinia Toolunun Kullanımı

Bu işlemden sonra Saldırgan (Kali) makinenin bağlı olduğu port Trunk moda geçti dolayısı ile tüm vlanlara erişim hakkı elde etti.



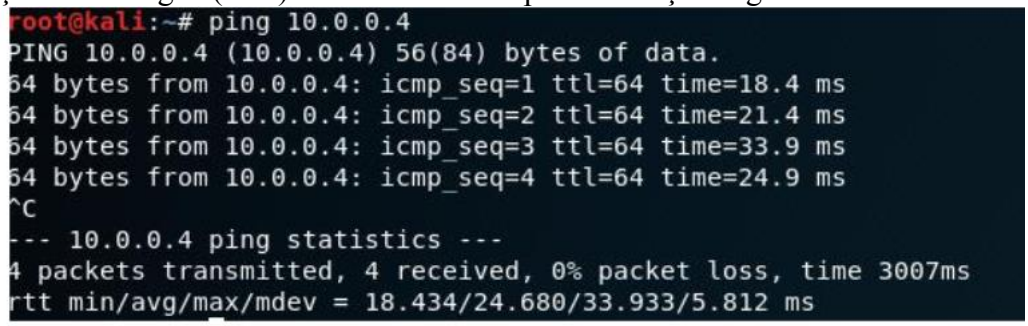
Şekil 12. İşlem Sonrası Switch Tarafındaki Vlan Gösterimi

Kali Linux makinesine aşağıdaki komut yazılır.



Şekil 13. Vlan Hopping için Kali Linux Komutu

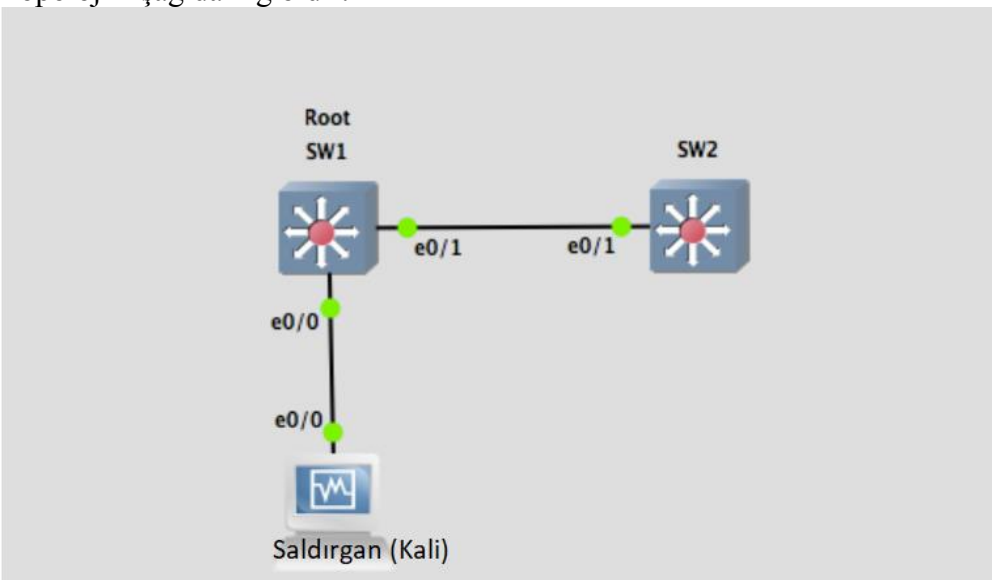
Şimdi Saldırgan (Kali) makinesinde tüm portlara erişim sağlanmaktadır.



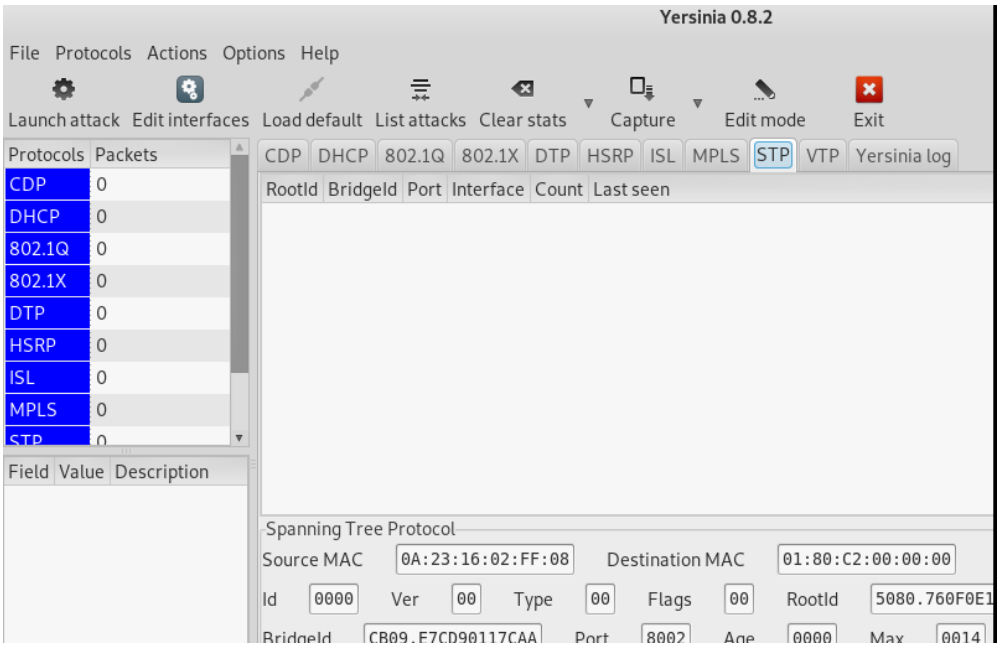
Şekil 14. İşlem Sonrası Farklı Vlanlarda Olan Kali ile PC-2 Arasındaki Ping Sonucu

5.3 Spanning-Tree Protokolü (STP) Saldırısı

Bu saldırı için Kali Linuxda bulunan Yersinia Toolu kullanılacaktır.
Topoloji Aşağıdaki gibidir.

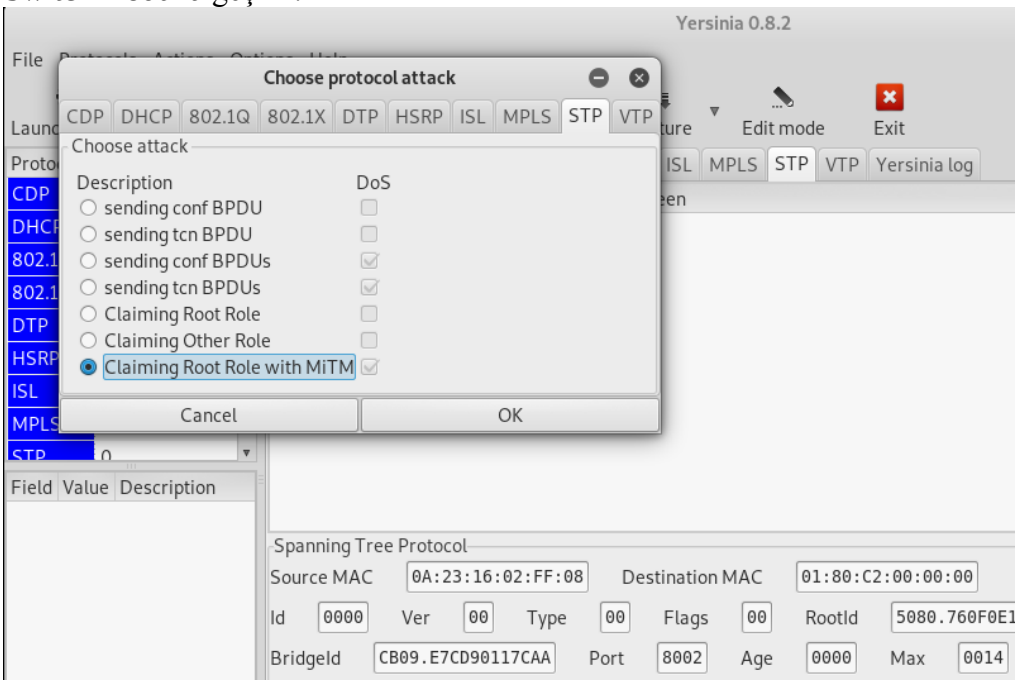


Şekil 15. Genel Topoloji



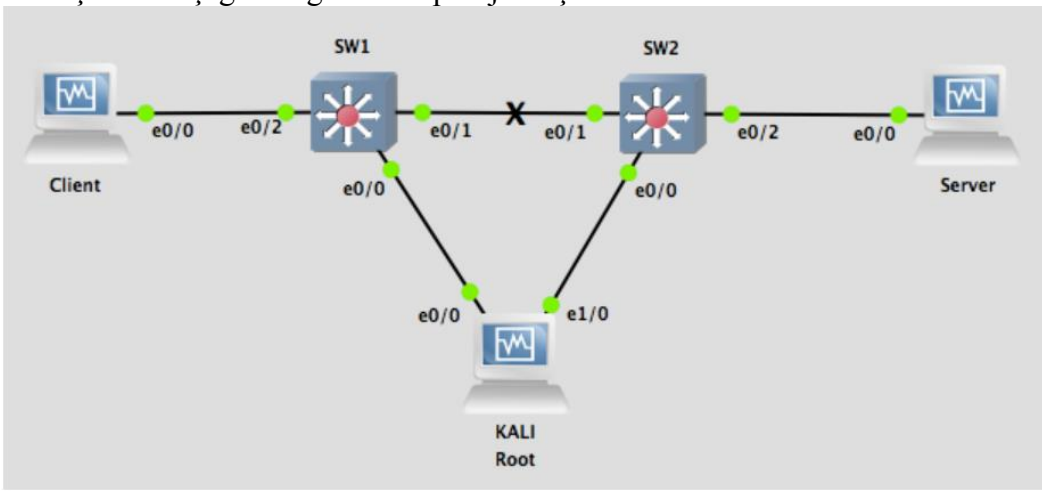
Şekil 16. Yersinia Arayüzü: Saldırı İçin Kullanılacak Araç

Saldırgan (Kali) Yersinia ile kendi BPDU değerini küçük gönderip Root Switch moduna geçilir.



Şekil 17. Yersinia Kullanımı

Son aşamada aşağıdaki gibi bir topoloji oluşmaktadır.



Şekil 18. Saldırı Sonrası Gösterim

Client ile Server arasında geçen trafik Saldırgan (Kali) üzerinde geçmektedir. Dolayısı ile trafik dinlenebilmektedir.

5.4 Sahte Mac (Mac Spoofing) Atağı

Sahte Mac saldırısı için Macchanger aracı kullanılacaktır.

```
root@kali:~#
root@kali:~# macchanger -h
GNU MAC Changer
Usage: macchanger [options] device

  -h,  --help                  Print this help
  -V,  --version               Print version and exit
  -s,  --show                  Print the MAC address and exit
  -e,  --ending                Don't change the vendor bytes
  -a,  --another               Set random vendor MAC of the same kind
  -A                           Set random vendor MAC of any kind
  -p,  --permanent             Reset to original, permanent hardware MAC
  -r,  --random                Set fully random MAC
  -l,  --list[=keyword]        Print known vendors
  -b,  --bia                   Pretend to be a burned-in-address
  -m,  --mac=XX:XX:XX:XX:XX:XX
       --mac XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
root@kali:~#
```

Şekil 19. Macchanger Kullanımı

Rastgele Mac Adresi için macchanger -r eth0 komutu ile rastgele mac adresi atması yapılabilir.

```
root@kali:~# macchanger -r
GNU MAC Changer
Usage: macchanger [options] device

Try `macchanger --help' for more options.
root@kali:~# macchanger -r eth0
Current MAC:   00:0c:29:d5:12:4e (VMware, Inc.)
Permanent MAC: 00:0c:29:d5:12:4e (VMware, Inc.)
New MAC:       8e:fc:25:29:86:08 (unknown)
root@kali:~#
```

Şekil 20. Macchanger ile Rastgele MAC Ataması

Kurban PC'ye gönderilen verileri elde etmek için "macchanger -m XX:XX:XX:XX:XX:XX eth0" ile hedef bilgisayarın Mac adresi yazılır.

```
root@kali:~# macchanger -m 8e:fc:25:29:86:10 eth0
Current MAC:   8e:fc:25:29:86:08 (unknown)
Permanent MAC: 00:0c:29:d5:12:4e (VMware, Inc.)
New MAC:       8e:fc:25:29:86:10 (unknown)
root@kali:~#
```

Şekil 21. Macchanger ile MAC Atamasının Yapılması

Bu işlemden sonra switchin Mac adres tablosunda aynı mac adresinde iki adet PC bulunacaktır. Bundan dolayı kurbana gidecek trafik saldırgana gönderilmiş olacaktır.

5.5 Sahte ARP (ARP Spoofing, ARP Poisoning) Atağı Uygulaması

Bu saldırı için Kali Linux'teki arpspoof aracı kullanılacaktır. Arpspoof kullanımı aşağıdaki gibidir.

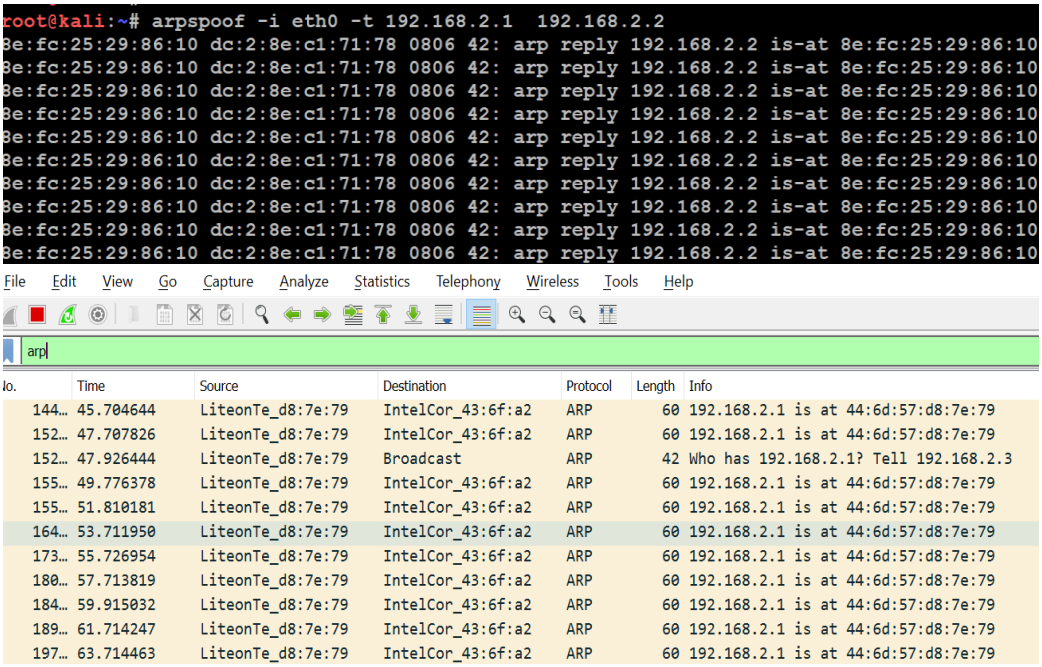
```
root@kali:~# arpspoof -h
Version: 2.4
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host
root@kali:~#
```

Şekil 22. Arpspoof Kullanımı

Bu saldırı şeklinde saldırgan kendini router yerine koyar ve tüm trafiğin kendi üzerinde geçmesini sağlar.

```
root@kali:~#
root@kali:~# arpspoof -i eth0 -t 192.168.2.2 192.168.2.1
8e:fc:25:29:86:10 f8:63:3f:43:6f:a2 0806 42: arp reply 192.168.2.1 is-at 8e:fc:2
5:29:86:10

8e:fc:25:29:86:10 f8:63:3f:43:6f:a2 0806 42: arp reply 192.168.2.1 is-at 8e:fc:2
5:29:86:10
8e:fc:25:29:86:10 f8:63:3f:43:6f:a2 0806 42: arp reply 192.168.2.1 is-at 8e:fc:2
5:29:86:10
8e:fc:25:29:86:10 f8:63:3f:43:6f:a2 0806 42: arp reply 192.168.2.1 is-at 8e:fc:2
5:29:86:10
8e:fc:25:29:86:10 f8:63:3f:43:6f:a2 0806 42: arp reply 192.168.2.1 is-at 8e:fc:2
5:29:86:10
8e:fc:25:29:86:10 f8:63:3f:43:6f:a2 0806 42: arp reply 192.168.2.1 is-at 8e:fc:2
5:29:86:10
8e:fc:25:29:86:10 f8:63:3f:43:6f:a2 0806 42: arp reply 192.168.2.1 is-at 8e:fc:2
5:29:86:10
8e:fc:25:29:86:10 f8:63:3f:43:6f:a2 0806 42: arp reply 192.168.2.1 is-at 8e:fc:2
5:29:86:10
8e:fc:25:29:86:10 f8:63:3f:43:6f:a2 0806 42: arp reply 192.168.2.1 is-at 8e:fc:2
5:29:86:10
8e:fc:25:29:86:10 f8:63:3f:43:6f:a2 0806 42: arp reply 192.168.2.1 is-at 8e:fc:2
5:29:86:10
```

Şekil 23. Arpspoof Kullanımı (2)



Şekil 24. Saldırı sonrası Wireshark görüntüsü

6. SONUÇLAR VE ÖNERİLER

Bu çalışmada iç ağda yapılabilecek saldırılar hakkında genel bilgiler verilmiştir. Ayrıca bu saldırıları bertaraf etmek için alınacak önlemler hakkında genel bilgiler verilmiştir. Sonraki araştırmacılar;

a. Türkiye'deki USOM ile siber güvenlik konusunda iyi durumda olan diğer ülkelerin USOM benzeri yapıların karşılaştırılması,
b. Ülke çapında kritik önemde bulunan kurumsal yapılarda siber güvenlik stratejilerinin karşılaştırılması,
c. Ülkemizdeki kritik yapılardaki kurumların siber güvenlik adına alınan önlemler ile siber güvenlik konusunda iyi durumda olan diğer ülkelerin kritik yapıların almış oldukları önlemlerin karşılaştırılması
d. Layer 2 de yapılan saldırılara karşı yukarda belirtilen önlemlere ek yeni önlemler,
e. Yapay sinir ağları ve benzeri yöntemler ile saldırıların tespitinin yapılması,
f. Tespit edilen saldırılara karşı otomatik işlem yapılması konularında araştırma yapabilir.

KAYNAKLAR

1. Halil BAYRAK, 2019 Dünya İnternet, Sosyal Medya ve Mobil Kullanıcı İstatistikleri erişim:30.01.2020 https://dijilopedi.com/2019-internet-kullanimi-ve-sosyal-medya-istatistikleri/
2. 2016-2019 Ulusal Siber Güvenlik Stratejisi, Erişim:31.01.2020 https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf
3. 2018 Sonicwall Siber Tehdit Raporu, Erişim 30.01.2020, http://www.m2s.com.tr/bulten/2018_Sonicwall_siber_tehdit_raporu-TR.pdf
4. Djamel Khadraoui, Francine Herrmann. "Advances In Enterprise Information Technology Security", Published in the United States of America by Information Science Reference, vol.1, pp. 1–19. (2007). http://api.wl2.stage.ovdal.dk/download.php?q=advances-in-enterprise-information-technology-security.pdf
5. Atıf Ünaldı, "***Netizen İnternet Vatandaşı***", Alt kitap yayınları, Cilt No:1, s.10, (2003) https://stratejikoperasyon.files.wordpress.com/2014/05/netizen.pdf
6. What Is Cybersecurity, erişim: 30.01.2020, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
7. USOM Hakkında, erişim:30.01.2020, https://www.usom.gov.tr/hakkimizda.html
8. USOM ve Kurumsal Siber Olaylara Müdahale Ekibi, erişim:30.01.2020, https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi
9. OSI Katmanları, erişim: 30.01.2020, http://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/osi-katmanlar%C4%B1
10. OSI Modeli Erişim: 30.01.2020, https://tr.wikipedia.org/wiki/OSI_modeli#4._Katman:_Ta%C5%9F%C4%B1ma/iletim_Katman%C4%B1

BÖLÜM3

KARARLILIĞIN ELEKTRİK DEVRELERİNDE BİLGİSAYAR DESTEKLİ ANALİZİ

Dr. Hasan CANGİ
Dr. Öğr. Üyesi Süleyman ADAK
Doç. Dr. Cemil İNAN

KARARLILIĞIN ELEKTRİK DEVRELERİNDE BİLGİSAYAR DESTEKLİ ANALİZİ[1]

Hasan CANGİ
Dr., HASCAN Mühendislik, Mardin

Süleyman ADAK
Dr. Öğr. Üyesi ,Mardin Artuklu Üniversitesi, Meslek Yüksekokulu, Elektrik ve Enerji Bölümü

Cemil İNAN
Doç. Dr.,Mardin Artuklu Üniversitesi, İktisadi ve İdari Bilimler Fakültesi İşletme Bölümü

1. GİRİŞ

Günümüzde bilgisayar destekli devre analizi oldukça kullanılmaktadır. Bu analiz işleminde en sık kullanılan programlardan biri Matlab programıdır. Matlab mühendislik alanında (hesaplamalarında); sayısal hesaplama, veri çözümleri ve grafik işlemlerinde kullanılabilecek genel amaçlı bir program olmakla beraber özel amaçlı modüler paketlere de sahiptir. Control Toolbox, SignalToolbox gibi paket programlar (Bilgisayar destekli denetim sistemi tasarımı) paketler olup bunlar denetim sistemlerinin tasarımında çok etkili araçlardır (Biran, 1995; Barrade, 2001). Ayrıca Windows ortamında çalışan Simulink, etkileşimli benzetim programlarının hazırlanması ve çalıştırılmasında büyük kolaylıklar sağlamaktadır. Basit bir diferansiyel denklem 'den bağımsız bir değişkene bağlı olduğu adi diferansiyel denklemdir. Komut içinde d/dt ifadesi "D" ile temsil edilir. Bu komutun çözümünden elde edilen fonksiyon içinde bir sabit bulunması istenmiyorsa bu durumda başlangıç koşullarını program içinde belirtilmesi gerekir. Aksi takdirde çözüm fonksiyonu sabitleri bulunduracaktır (Tokad, 1987; Chua, vd.1987; Altıntaş, 2006).

[1] Bu çalışma "Mardi Artuklu 3.Bilimsel Araştırmalar Sempozyumunda Sunulmuştur

A: n*n tipinde reel sayıların bir matrisi olmak üzere, λ ya göre bir polinom denklemi olan, det(A-λ I)=0

denklemine A nın karakteristik denklemi ve köklerine A'nın özdeğerleri denir. λ nın bir polinomu olup, bu polinoma T nin karakteristik polinomu denir.

$$T(\lambda) = |A - \lambda I| = 0$$

denklemine de karakteristik denklem denir.Bir elektrik devresinde kararlılık şartı sisteme ilişkin özdeğerlerin kompleks düzlemde sol yarı tarafta bulunması ve varsa sanal düzlemde özdeğerlerin katsız olmasıdır (Skaar, 2001; Samosir, vd., 2010;Astrom, 1990).

Matlab programının kullanım yerleri:

- Denklem takımlarının çözümü, doğrusal ve doğrusal olmayan diferansiyel denklemlerinin çözümü, integral hesabı gibi sayısal hesaplamalar,
- Veri çözümleme işlemleri,
- İstatistiksel hesaplamalar ve çözümlemeler,
- Grafik çizimi ve çözümlemeler,
- Bilgisayar destekli denetim sistemi tasarımı.

2. ARAŞTIRMA

Elektrik devrelerinin kararlılık analizinde Matlab programlama dili yoğun bir şekilde kullanılmaktadır. Matlab programı ile karışık matematiksek problemlerin kolayca çözümünden üç boyutlu eğri çizimine kadar çok geniş alanda mükemmel sonuçlar veren ve öğrenimi diğer programlama dillerine göre çok basit olan bir yazılımdır. Matlab, komut temelli bir programdır. Matlab'da Matrisler ile İlgili kullanılan Özel Komutlar:

- Matrisin Determinantının Alınması: Matlab **det** komutu
- Matrisin Rankının Alınması: Matlab **rank** komutu
- Matrisin İzinin Bulunması: Matlab **trace** komutu
- Matrisin Tersinin Bulunması: Matlab **inv** komutu
- Matrisin Karakteristik Denkleminin Bulunması: Matlab **poly** komutu
- Matrisin Özdeğer ve Özvektörlerinin Bulunması: Matlab **eig** komutu

- Matrisin Ortogonal Matrisinin Bulunması: Matlab **orth** komutu

Komutları kullanılır. Bir A Matrisinin öz değerleri **eig**(A) Matlab komutu ile bulunur. Bir A matrisi aşağıdaki gibi verilsin.

$$A=\begin{bmatrix} 1 & 4 & 7 \\ -2 & 5 & -8 \\ 3 & 6 & 1 \end{bmatrix} \qquad (1)$$

»A = [1 4 7; -2 5 -8; 3 (2)

»Ozdegerler=eig(A) (3)

Özdeğeler,

λ_1= -2.9650

λ_2= 4.9825 + 7.1219i

λ_3=4.9825 - 7.1219i

Simulink matlab ile ortak bir şekilde kullanılabilir. Elektrik devrelerinde durum denklemlerindeki durum değişkenlerinin sayısına o devrenin karmaşıklık mertebesi adı verilir. Durum değişkenleri ise seçilen ağaç yapısına göre dallardaki kondansatörlerin gerilimleri ile kirişlerdeki endüktansların akımlarıdır. n.ci mertebeden bir devrenin durum denklemlerinin genel yapısı, aşağıdaki diferansiyel denklem sistemi gibidir.

$$\frac{d}{dt}\begin{bmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_n(t) \end{bmatrix} = A\begin{bmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_n(t) \end{bmatrix} + B\mathbf{u}(t) \qquad (4)$$

Burada $x_1(t)$, $x_2(t)$ …. $x_n(t)$ terimleri dal kapasite gerilimleri ve kiriş endüktansakımlarıdır. A ve B matrislerinin elemanları devredeki direnç, kapasite ve endüktans gibi elemanların değerlerinin fonksiyonlarıdır(Attia, 2004; Acar, 1999; Kubat, 2015). $\mathbf{u}(t)$ vektörü ise

kaynaklara ilişkin değerleri içerir. Durum denklemlerinin çözümleri incelenirken, çözüm ifadelerinde iki ayrı terim bulunmaktadır. Bunlardan ilki, devrede kaynaklar yokken, kapasitelerin ilk gerilimleri ve endüktansların0 ilk akımları nedeniyle ortaya çıkan, devrenin öz çözümüdür(Nasar, 1989;Nilsson, vd. 2005;Boylestad, 2010). İkinci terim ise, devrede bulunan kaynaklar nedeniyle elde edilen, devrenin zorlanmış çözümüdür. Tam çözüm, öz ve zorlanmış çözümün toplamıdır.

$$\mathbf{x_{tam}}(t) = \mathbf{x_{öz}}(t) + \mathbf{x_{zorlanmş}}(t) \qquad (5)$$

Elde edilen diferansiyel denklem sisteminin çözümü şu şeklindedir.

$$\mathbf{x}(t) = \Phi(t)\mathbf{x}(0) + [\mathbf{x_{ö}}(t) - \Phi(t)\mathbf{x_{ö}}(0)] \qquad (6)$$

Bu çözümde $t \to \infty$ için $\Phi(t) \to 0$ oluyorsa, öz çözüm sıfıra, zorlanmış çözüm de özel çözüm $\mathbf{x_{ö}}(t)$'ye uzanmaktadır. Bu özelliğe sahip olan devrelere asimptotik kararlı devreler adı verilir. Asimptotik olarak kararlı bir devrenin öz çözümü $\mathbf{x_h}(t)$ geçici çözüm; özel çözümü $\mathbf{x_{ö}}(t)$ sürekli çözüm adını almaktadır (Arifoğlu, 2016).

Özdeğerler ve özvektörler, diferensiyel denklemler içeren denklem sistemlerinin çözümlerinde, sınır-değer problemlerinde ortaya çıkabilir. Bu tür denklemlere, doğru akım devrelerinde titreşim yapan cisimlerin hareketlerinde sıkça karşılaşılır. Titreşim yapan bir sistemin doğal frekansı ile dışarıdan uygulanan sürücü kuvvetin frekansı birbirine eşit veya yakın olması sistemin kararlılığı açısından önemli olmaktadır. Durum denklemlerinde bulunan A matrisine ait özdeğerler "det(A- λ I)=0" ifadesinden bulunur. Burada, λ, öz değerleri, I, birim matrisi göstermektedir.

ÖRNEK-1

Aşağıda durum denklemi verilen elektrik devresinin kararlılığını inceleyelim.

$$\frac{d}{dt}\begin{bmatrix} V_C \\ i_L \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ -2 & 0 \end{bmatrix}\begin{bmatrix} V_C \\ i_L \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} U(t) \qquad (7)$$

Devrenin A matrisi aşağıda verildiği gibidir.

$$A = \begin{bmatrix} -1 & -1 \\ -2 & 0 \end{bmatrix} \qquad (8)$$

Devrenin özdeğerleri,

$$\det(A - \lambda I) = 0 \qquad (9)$$

$\lambda 1 = -2$ ve $\lambda 2 = 1$

Köklerden biri olan "1" sağ yarı düzlemde olduğu için elektrik devresi kararsızdır.

ÖRNEK-2

Aşağıda durum denklemi verilen elektrik devresinin kararlılığını inceleyelim.

$$\frac{d}{dt}\begin{bmatrix} V_C \\ i_L \end{bmatrix} = \begin{bmatrix} -2 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} V_C \\ i_L \end{bmatrix} + \begin{bmatrix} 8 \\ 0 \end{bmatrix} U(t) \qquad (10)$$

Elektrik devresinin A matrisi,

$$A = \begin{bmatrix} -2 & -1 \\ 1 & 0 \end{bmatrix} \qquad (11)$$

Devrenin özdeğerleri,

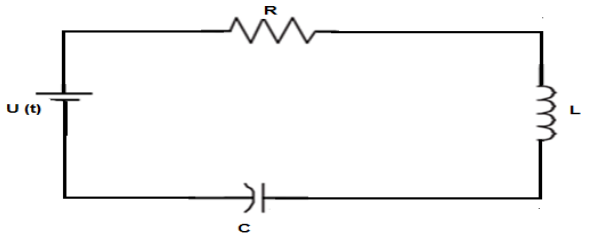
$$\det(A - \lambda I) = 0 \qquad (12)$$

$$\lambda_1 = -3.7321 \text{ ve } \lambda_2 = -0.2679$$

Özdeğerler sol yarı düzlemde olduğundan devre karalıdır.

2.1 Elektrik Devrelerinde Kararlılığın Matlab Programı Komutları İle Analizi

Devreler karmaşık hale geldikçe (örneğin kaynak sayısı birden fazla ise ve birden fazla değişkenin aynı anda incelenmesine ihtiyaç duyulursa)yani devreler çok girişli ve çok çıkışlı hale geldiğinde bu devrelerin diferansiyel denklemleri yerine durum denklemlerini çıkarmak daha kolay hale gelir. Şekil 1'de analiz işleminde kullanılacak doğru akım ve RLC elemanlarından oluşan devre.



Şekil 1. Doğru akım ile sürülen RLC devresi

Şekil 1'deki devreye ilişkin durum denklemleri diferansiyel denklem formundadır. dsolve komutu basit diferansiyel denklemler çözülebilir. Basit diferansiyel denklem bilinmeyen fonksiyonun sadece bir bağımsız değişkene bağlı olan adi diferansiyel denklemlerdir. Matlab genel olarak, Matematiksel işlemler, Algoritma geliştirme, Veri analizi 2 ve 3 boyutlu grafik çizimlerinde, Dinamik sistemlerinin simulink modellerinin çıkarılmasında kullanılır."eig" komutunun elektrik devrelerinde devrenin kararlığının incelenmesinde kullanılır. Günümüz ekonomik koşulları dikkate alındığında laboratuar kurmanın zorluğu karşısında sistemlerin simulink karşılıklarını oluşturup bilgisayar destekli analiz edilmeleri gün be gün önem kazanmaktadır. Matlab komut içinde d/dt türev operatörü " D" ile gösterilir. Bu komutun çözümünden elde edilen fonksiyon içinde bir sabit bulunması istenmiyorsa başlangıç koşullarını program içinde belirtilmesi gerekir. dsolve: Diferansiyel denklemlerin sembolik

çözümünü verir. Örneğin, D^2y; y' nin ikinci türevi, Dy ise y' nin birinci türevini ifade eder. Kondansatör akımı,

$$C\frac{dv_C(t)}{dt} = i_C(t) \tag{13}$$

Endüktans gerilimi,

$$L\frac{di_L(t)}{dt} = V_L(t) \tag{14}$$

Olarak bulunur. Kondansatör akımı endüktans akımına eşit olduğundan,

$$i_c = i_L \tag{15}$$

$$\frac{dV_c}{dt} = \frac{1}{C}i_L \tag{16}$$

Devrenin çevre denklemini yazarsak,

$$V_R + V_L + V_C = U(t) \tag{17}$$

$$\frac{di_L}{dt} = \frac{1}{L}U(t) - Ri_L - V_c \tag{18}$$

Durum denklemlerini matrissel formda yazmakla sisteme ilişkin işaret akış diyagramına geçiş yapılabilir. Aynı zamanda durum denklemlerinden hareketle sistemlerin Simulink modelleri oluşturulabilir. Lineer kontrol sistemlerinin, en önemli konularından biri kararlılıktır. Sistemin, hangi koşullar altında kararsız olduğu ve eğer kararsızsa, sistemin kararlı hale nasıl getirilebileceği konularına oldukça dikkat edilmelidir. Bulunan denklemleri matrissel formda yazarsak,

$$\frac{d}{dt}\begin{bmatrix} V_C \\ i_L \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{C} \\ -\frac{1}{L} & -\frac{R}{L} \end{bmatrix}\begin{bmatrix} V_C \\ i_L \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{L} \end{bmatrix}U(t) \tag{19}$$

Elektrik devrelerini ait durum denklemlerini matrissel formda yazmakla bilgisayar destekli analiz yapmak imkanıelde edilir. Günümüzde matrisleri Matlab yazılım programı yardımı ile kolaylıkla çözebiliriz. C=1/50F, L=1/100H ve R=10 ohm değerleri için,

$$\frac{d}{dt}\begin{bmatrix} V_C \\ i_L \end{bmatrix} = \begin{bmatrix} 0 & 50 \\ -100 & -1000 \end{bmatrix}\begin{bmatrix} V_C \\ i_L \end{bmatrix} + \begin{bmatrix} 0 \\ 100 \end{bmatrix} U(t) \quad (20)$$

Olarak bulunur. Devrenin öz değerleri,

$$\det(A - \lambda I) = 0 \quad (21)$$

λ_1=-5.0253 ve λ_2 =-994.9747

Olarak bulunur.Özdeğeler sol yarı düzlemde olduğundan devre kararlıdır. Matlab komutları ile kararlılığı incelersek,

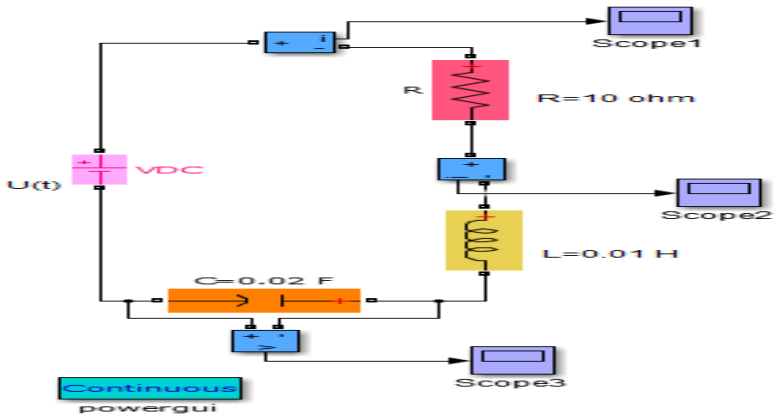
```
>> A=[0 50;-100 -1000];          (22)
>>eig(A)                        (23)

ans =

λ1= -5.0253 ve  λ2= -994.9747
```

Olarak bulunur. Özdeğeler sol yarı düzlemde olduğundan devre kararlıdır. Matlab/Simulink yardımı ile zor olan teknik problemleri kolay, zahmetsizce ve aynı zamanda görsel olarak çözmek mümkündür. Günümüzde laboratuvar kurmanın zorluğu karşısında sistemlerin Simulink modellerinin kurulup bilgisayar destekli analiz edilmeleri gün be gün önem kazanmaktadır.

2.2 Matlab/Simulink ile RLC Devresinin Analizi

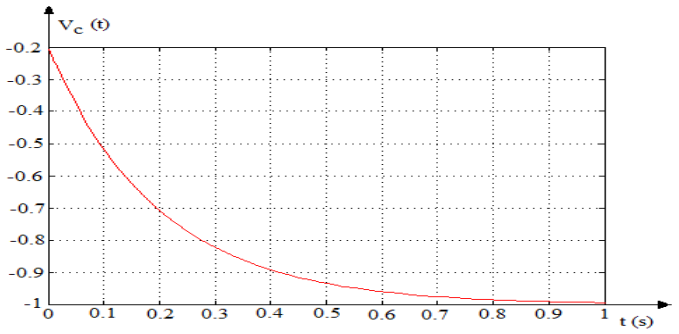
Doğrusal ve zamanla değişmeyen sistemlerin matematiksel modelleri; diferansiyel denklemler, transfer fonksiyonları ya da durum denklemi düzeninde elde edilebilir. Ancak, kontrol sistemlerinin analiz ve tasarımında transfer fonksiyonu gösterimi önemli kolaylıklar sağlar. Matlab kontrol sistemleri toolbox' ında transfer fonksiyonlarının bir

gösterim biçiminden diğer gösterim biçimine dönüşümünü ve durum denklemleri ile dönüşümünü sağlayan fonksiyonlar mevcuttur. Ayrıca, transfer fonksiyonu ve durum denklemi ile modellenen sistemlerin basamak, impuls ve çeşitli giriş sinyalleri için cevabını bulan fonksiyonları da bulunmaktadır. Matlab/Simulink yardımı ile zor olan teknik problemleri kolay, zahmetsizce ve aynı zamanda görsel olarak çözmek mümkündür. Laboratuar kurmanın zorluğu karşısında sistemlerin Simulink modellerinin kurulup bilgisayar destekli analiz edilmeleri gün be gün önem kazanmaktadır. R=10 ohm, C=1/50 F ve L=1/100 H, $i_L(0)$=0.1 A, $V_c(0)$=0.2 V değerlerinde verilen doğru akım RLC devresinin Simulink eşdeğeri Şekil 2'de verilmiştir.



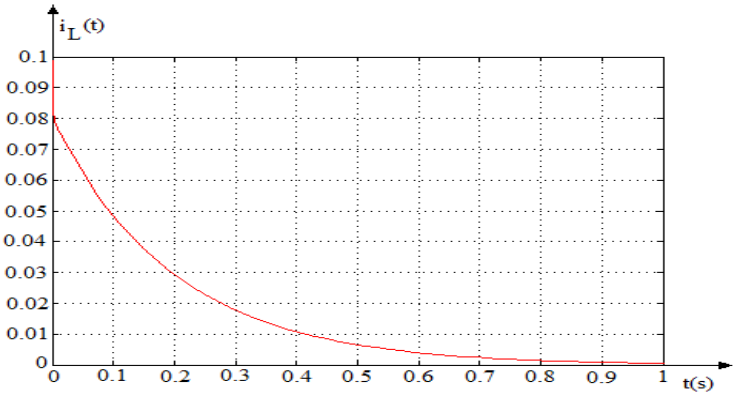
Şekil 2. Doğru akım ve RLC elemanlarından oluşan devrenin Simulink eşdeğeri

Simülasyon neticesinde, tasarlama zamanı, montaj fiyatında azalmalar oluşur. Sistemlerin kombine olarak tasarlanması sistem analizini ve parametrelerde geniş sınırlar içinde değişikliğe gidilmesi kolaylığını getirmektedir. Devrelerin simülasyon eşdeğerlerinin oluşturulması neticesinde, tasarlama zamanı, montaj fiyatında azalmalar oluşur. Sistemlerin kombine olarak tasarlanması sistem analizini ile devre parametrelerde geniş sınırlar içinde değişikliğe gidilmesi kolaylığını getirmektedir. Şekil 3'te kondansatör gerilimin zamana bağlı değişimi verilmiştir.



Şekil 3. Durum değişkeni olarak kondansatör gerilimin değişimi

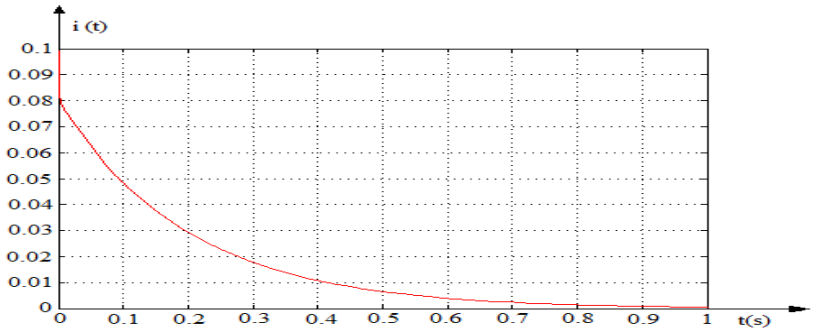
Doğru akım devrelerinin Simulink modellerinin oluşturulması ile bilim ve teknolojiye dayalı yeni fikir ve buluşların sisteme yansıtılması sağlanabilir. Sistemlerin titreşimli veya aşırı sönümlü olduklarını transfer fonksiyonuna birim basamak fonksiyonu uygulanarak öğrenilebilir. Simülasyon çalışmaları laboratuvar çalışmaları ile desteklenmelidir. Matlab programı genel, Matematiksel işlemler, Algoritma geliştirme, Veri analizi 2 ve 3 boyutlu grafik çizimlerinde, Dinamik elektrik sistemlerinin Simulink modellerinin oluşturulmasında oldukça kullanışlı bir programlama dilidir. Simulink desteği Matlab'a ayrı bir avantaj kazandırmıştır. Şekil 4'te durum değişkeni endüktans akımının değişimi verilmiştir.



Şekil 4. Durum değişkeni olarak endüktans akımının değişimi

Simülasyon neticesinde, tasarlama zamanı, tasarım fiyatında azalmalar oluşur. Sistemlerin kombine olarak tasarlanması analizi ve parametrelerde geniş sınırlar içinde değişikliğe gidilebilir. Simülasyon modellemesinde yazılım ve donanım birlikte kullanılabilir. Matlab programlama dili, çok

karışık matematiksek problemlerin kolayca çözümünden üç boyutlu eğri çizimine kadar çok geniş alanda mükemmel sonuçlar veren ve öğrenimi diğer programlama dillerine göre çok basit olan bir yazılımdır. Şekil 5'te devre akımının zamana bağlı değişimi verilmiştir.



Şekil 5. Devren akan akımın değişimi

Sistemlere ilişkin simülasyonunu benzetimi sonucunda devre parametrelerinin geniş sınırlar içinde değiştirme imkânına mevcuttur. Sistem optimal şartları sağlayana kadar değişiklikler yapılabilir. Sistemlerin tasarımında büyük oranda bilgisayar simülasyonlarından faydalanmakta, mümkün olduğunda tasarımın test aşamaları da bilgisayarlar yardımıyla yapılmaktadır. Günümüz koşullarında bilgisayar desteği almayan çalışmaların güvenilirliği oldukça azdır. C++, Basic veya Fortran dilinde satırlarca işlem yaparak ulaşabileceğimiz sonuçlara Matlab programında 2-3 komutla ulaşabiliriz.

3. SONUÇLAR

Bu çalışmada doğru akımda RLC devresinin durum denklemleri çıkarılıp sistemin kararlılık analizi yapılmıştır. Doğru akım devresinde kararlılık analizinin yapıldığı bu çalışmanın genel sonucu olarak, şunlar söylenebilir:

- Kararsız dinamik devrelerde durum değişkenleri endüktans akımı ile kapasite gerilimi sonsuz değerler alır. Endüktans akımı aşırı değerinden dolayı yanar kapasite elemanı ise aşırı gerilimden dolayı dielektirik kısmı delinir. Bundan dolayı fiziksel olarak gerçekleştirilen devrelerde kararlılık analizi çok önemlidir.

- Doğru akım RLC elemanlarından oluşan doğru akım devresinin klasik yöntemlerle kararlılık analizinin yapılması oldukça zordur. Bu devrelerin durum denklemlerini çıkarıp, Matlab yazılım programı komutları kullanılarak devrenin kararlılık analizinin bilgisayar destekli yapmak oldukça kolaydır.
- Elektrik devrelerinin simülasyon modellemelerinde yazılım ve donanım birlikte kullanılabilir. Sistemlerin simülasyonu neticesinde tasarımında talep değişikliklerine daha kolay cevap verilebilir. Teknolojik yeniliklerin sisteme adaptasyonu kolaylıkla yapılabilir.

4. KAYNAKLAR

Biran, A. Breiner, M. (1995) Matlab for Engineers, Addison-Wesley Pub. Comp.

Barrade, P. (2001) Simulation Tools for Power Electronics: Teaching and Research". SIMPLORER Workshop 2001. Chemnitz. pp.35-46.

Tokad, Y. (1987) Devre Analizi Dersleri – Kısım 4, , Çağlayan Kitabevi.

Milano, F. (2005) An Open SourcePowerSystem Analysis Toolbox, IEEE Transactions on PowerSystems, 20(3), 1199-1206.

Chua, L.O. Desoer, C.A. S.E. Kuh.S.E.(1987) LinearandNon-linearCircuits, McGraw-Hill.

Altıntaş, A. (2016) Matlab ve Genel Uygulamaları, Değişim yayınları, İstanbul.

Skaar, D. L. (2001) Using thesuperpositionmethodtoformulatethestatevariablematrixforlinearnetworks, IEEE Trans. Educ.,vol. 44, no. 4, pp. 311–314, Nov.

Samosir, A. S. Yatim, A.H. (2010) Implementation of DynamicEvolution Control of Bidirectional DC-DC Converter forInterfacingUltracapacitorEnergy Storage toFuel Cell System, IEEE Trans IndustrialElectronics, Vol 57, No.10, Oct 2010, pp 3468-3473

Astrom, K. J. Wittmenmark, B. (1990)ComputerControlledSystems, 2nded.EnglewoodCliffs, NJ: Prentice-Hall.

Attia, J. O. (2004) Electronics and Circuit Analysis Using Matlab. Boca Raton, FL: CRC Press.

Acar, C. (1999) Elektrik Devrerelerinin Analizi, İTÜ, Elektrik –Elektronik Fakültesi, Ofset Baskı Atölyesi, İstanbul.

Kubat, C. (2015)n Matlab, Yapay Zeka ve Mühendislik Uygulamaları, Vakademi, İstanbul.

Yüksel, İ. (2000) MATLAB ile Mühendislik Sistemlerinin Analizi ve Çözümü, Genişletilmiş II. Baskı", Vipaş A.Ş., Bursa.

Nasar, S. A. (1989), Schaum's 3000 SolvedProblemsinElectricCircuits, McGraw-HillBookCompany.

Nilsson, J. W.,Riedel, S. A. (2005), ElectricCircuits,Prentice-Hall.

Boylestad, R. L. (2010). IntroductoryCircuit Analysis. PrenticeHall.

Arifoğlu, U (2016) MATLAB 9.1Simulink ve Mühendislik Uygulamaları, 1. Baskı. İstanbul.

BÖLÜM4

DÖNER KANATLI HAVA ARAÇLARININ UÇUŞ PERFORMANS OPTİMİZASYONU

Öğr. Gör. Hüseyin ŞAHİN
Doç. Dr. Tuğrul OKTAY
Dr. Ögr. Üyesi Mehmet KONAR

DÖNER KANATLI HAVA ARAÇLARININ UÇUŞ PERFORMANS OPTİMİZASYONU

Hüseyin ŞAHİN
Öğr. Gör.,Ankara Yıldırım Beyazıt Üniversitesi

Tuğrul OKTAY
Doç. Dr., Erciyes Üniversitesi

Mehmet KONAR
Dr. Ögr. Üyesi,Erciyes Üniversitesi

1. Giriş

Döner kanatlı hava araçları, arama kurtarma, denetleme ve ulaşım gibi kritik uygulamalarda kullanılmaktadırlar. Uygulamaların artmasıyla birlikte, bu hava araçlarının popülerlikleri de artmıştır. Kullanım sahasının gelişmesiyle, değişik görev taleplerini ortaya çıkarmıştır. Bu görev talepleri, kullanım süresinin ve menzili uygulama alanlarının sınırlanmasına neden olmuştur [1]. Sınırlı uçuş süresi ve menzil problemine yönelik, dikey kalkış ve iniş yapabilme kapasitesine sahip hava araçları ve hibrid çözümler gibi yeni olası çözümler üzerine çalışılmaktadır [2].

Hava araçlarının verimliliğinin arttırılması için sezgisel tabanlı optimizasyon yöntemleri, kolay uygulana bilirliği ve ekonomik yapısından dolayı sıklıkla tercihe edilmektedir. Bu yaklaşımlar aerodinamik ve itki tasarımlarından kullanılmaktadır. İtki tasarımında, batarya gücü, motor ve pervane verimliliği, hava aracının toplam ağırlığı, performans kayıpları, bulunduğu ortamın değişkenleri, hava aracının kullanım şekli ve hava aracının aerodinamik yapısı dikkate alınması

gereken parametrelerden bazılarıdır. Bu parametrelerden hava aracının toplam ağırlığı uçuş süresini ters orantılı olarak etkilerken, batarya kapasitesi doğru orantılı olarak etkilemektedir.

İtki sisteminde kullanılan bileşenlerin hava aracı ağırlığı üzerinde önemli bir etkisi vardır. Bu bileşenler temel olarak, pervane, motor, hız kontrol ünitesi (Electronic Speed Controller, ESC) ve bataryadan oluşmaktadır. Bu bileşenler itki sisteminin ortaya çıkardığı güce ve hava aracının ağırlığını etkilediğinden dolayı, uçuş performansını da doğrudan etkilemektedir [3]. Bununla birlikte, üretilen güç, asılı kalabilmesi için gereken güç ve taşıyabileceği faydalı yük miktarını da belirlemektedir. Döner kanatlı hava araçları faydalı yük olarak kamera, fotogrametri sistemleri, robot kol gibi cihazlar kullanılabilmektedir [4].

Bu çalışmada, elektrik tahrikli çok rotorlu döner kanatlı hava araçlarının düşük pil tüketimi için ağırlık yönetimi optimizasyonu için ön tasarımın incelenmesi yapılmıştır. Bataryanın farklı gerilim, akım, güce sahip olmasının ağırlığa uçuş süresine etkisi ile ilgisi bağlantı incelenmiştir [5-6].

2. Metot

Bir faydalı yüke sahip olan çok rotorlu döner kanatlı hava araçlarının itki sisteminde genellikle elektrikli motorlar kullanılmaktadır. Bu hava araçlarının %90'ında, yüksek güç, yüksek enerji yoğunluğuna ve düşük ağırlığa (diğer pil çeşitlerine göre) sahip olması nedeniyle lityum piller kullanılmaktadır.

İtki sistemi tasarım aşamalarında, hava aracının sağlıklı uçabilmesi için gerekli gücün hesaplanması ve batarya deşarj akımının hesaplaması dikkate alınan konuların başında gelmektedir. Gerekli gücün hesaplanmasında, hava aracının gerçekleştireceği görev ve hava aracının ağırlık dikkate alınır. Bu parametreler dikkate alınarak, pervane ve motor kombinasyonları seçilir ve gerekli güç hesaplaması yapılır. Daha sonra, gerekli güç hesaplamasıyla, bataryanın deşarj akımı bulunarak uçuş süresi tahmini yapılır [7]. Şekil 1’de döner kanatlı hava aracının tasarım sürecinin gösterimi verilmiştir.

Şekil 1. Döner kanatlı hava aracının tasarım aşamaları

3. Analiz

Elektrik enerjisi kullanarak uçan hava araçlarının boyutları ve uçuş süreleri sınırlıdır. Bu hava araçları özel bir uygulama için çok büyük olmalarının performansı düşmesine neden olacaktır. Bir hava aracının uçuş süresi, hava aracının ağırlığına, bataryanın kapasitesine ve enerji kullanımına bağlıdır [8]. Döner kanatlı hava aracına gereken güç, hava aracının ağırlığına ve pervane yarıçapına bağlıdır. Hava aracına gereken gücün formülü Eşitlik1'de verilmiştir.

$$P = \frac{T_h^{\frac{3}{2}}}{\sqrt{A}} = \frac{W^{\frac{3}{2}}}{r_p} \tag{1}$$

Örnek bir hava aracının ağırlığı 0,5 kg ve pervane yarıçapı 0.3 m olarak dikkate alınırsa, Eşitlik 1 de yerine koyarsak gereken gücün hesaplaması Eşitlik 2 ile gösterilmiştir.

$$P_h = \frac{T_h^{\frac{3}{2}}}{\sqrt{2qS}} = \frac{0,5^{\frac{3}{2}}}{\sqrt{2.1,225.0,3^2.\pi}} = 0,2549W \quad (2)$$

Aynı malzemelerden üretilen küçük bir hava aracının üretilecek olsa boyutunu iki faktörle küçültürsek, 3 boyuttan dolayı ağırlık $(1/2)^3$ yani 1/8 oranı ile azalır ve pervane yarıçapını yarıya indirirsek gerekli gücün değişimi Eşitlik 3'deki gibi hesaplanacaktır.

$$P_h = \frac{T_h^{\frac{3}{2}}}{\sqrt{2qS}} = \frac{(0,5/8)^{\frac{3}{2}}}{\sqrt{2.1,225.1,5^2.\pi}} = 0,0038W \quad (3)$$

Ancak bu değişim neticesinde bataryanın kapasitesi de 8 kat azalmış alacaktır. Büyük hava aracı 0,2549 Wh kapasiteye sahip batarya ile 1 saat uçabiliyor ise küçük hava aracının aynı malzemeden üretilen batarya ile uçuş süresi Eşitlik 4'deki gibi teoride 8,4 saat olarak bulunacaktır.

$$süre = \frac{0,2549/8}{0,0038} = 8,4s \quad (4)$$

Yani daha küçük hava aracı diğerine göre uçuş süresi %840 arttığı görülmüştür. Ya da tam tersi şekilde hava aracının boyutunu 2 kat artırırsak ağırlık 8 kat, pervane çapı ise 2 kat artar ve yeni hava aracının uçuşu için gerekli güç Eşitlik 5'de verilmiştir.

$$P_h = \frac{T_h^{\frac{3}{2}}}{\sqrt{2qS}} = \frac{(0,5x8)^{\frac{3}{2}}}{\sqrt{2.1,225.0,6^2.\pi}} = 4,8060W \quad (5)$$

Hava aracını 2 kat büyüttüğümüzde batarya kapasitesi de 8 kat artacağından büyük hava aracının uçuş süresi Eşitlik 6'daki gibi bulunacaktır.

$$süre = \frac{0,2549x8}{4,8060} = 0,4s \quad (6)$$

Büyük hava aracının uçuş süresi 0,4 saat olur yani hava aracının boyutunu 2 kat büyüttüğümüzde uçuş süresi %60 oranında düşecektir. Hava aracının boyutu büyüdükçe batarya kapasitesini de aynı oranda artırmış olsak bile uçuş süresi düştüğü görülmektedir.

Hava aracında ağırlık ölçümü

Hava aracının güç sistemini tasarlarken ağırlığının tahmini önemlidir. Güç sistemi hariç toplam ağırlığı ölçtükten sonra güç sistemindeki ağırlığın hesaplanabilmesi için bataryanın kütlesini hesaplamak gerekir [9]. Bataryanın ağırlığı hesaplamak için Eşitlik 7'den faydalanılmaktadır.

$$m_{bat} = \frac{c_{bat}.V_{bat}}{k_{bat}} \tag{7}$$

Formülde c_{bat} bataryanın kapasitesi, V_{bat} bataryanın voltajını, k_{bat} ise bataryanın katsayısını göstermektedir. Motor kütlesi ise Eşitlik 8 ile gösterilmiştir.

$$m_{motor} = P_{motor}.k_{motor} \tag{8}$$

Eşitlik 8'deki p_{motor}, motor gücünü, k_{motor} ise motor katsayısını belirtmektedir. İtki sisteminde kullanılan motor ve bataryanın ağırlığı hesaplanırken en önemli etkenler bu parçaların katsayılarıdır. Parça katsayıları üretim metotları ve üretildiği malzemelere bağlıdır. Motor ve batarya katsayıları ise bu parçaların üreticilerinin veri tabanından faydalanılarak bulunabilir. Diğer itki sisteminin ağırlığının en önemli ikinci parametresi ise itki sisteminde kullanılan parçaların güçleridir.

Havada kalış süresi optimizasyon işlemi, performans parametrelerinin hesaplanması ile gerçekleştirilir. Bu optimizasyon işleminin amacı havada kalış süresini artırmaktır. Tasarımda, geometrik parametreler, operasyon parametreleri (düz uçuş hızı) ve batarya kapasitesi değişken parametreleri oluşturmaktadır [14].

4. Sonuç

Bu çalışmada elektrik tahrikli döner kanatlı hava araçlarının menzil ve uçuş sürelerini tahmin etmek için gerekli ilişkiler belirlenmiştir. Hava aracının uçuş süresinin optimizasyonu için gerekli olan formüllerden ilki hava aracının boyutu ve gerekli olan minimum elektrik gücüdür. Hava aracı boyutunun uçuş süresine etkisi belirlenmiştir. Diğer formül ise itki sisteminin ağırlığıdır. İtki sisteminde kullanılan parçaların ağırlığı hesaplama formülleri ile birlikte toplam ağırlık ve gerekli güç değişecektir. Sonuç olarak hava aracının batarya kapasitesinin artırılması toplam ağırlığı da artıracağından havada kalış süresini her zaman artıramayabilir.

5. Kaynakça

1. Nonami, K., Kendoul, F., Suzuki, S., Wang, W., & Nakazawa, D. (2010). Autonomous flying robots: Unmanned Aerial Vehicles and Micro Aerial Vehicles. In Autonomous Flying Robots: Unmanned Aerial Vehicles and Micro Aerial Vehicles. https://doi.org/10.1007/978-4-431-53856-1
2. Chang, T., & Yu, H. (2015). Improving Electric Powered UAVs' Endurance by Incorporating Battery Dumping Concept. Procedia Engineering, 99, 168–179. https://doi.org/10.1016/j.proeng.2014.12.522
3. Srigrarom, S., Xiang, L. H., How, L. C., Yang, S. Z., & Wei, Z. J. (2015). Design and Build of Swarm Quadrotor UAVs. 15th AIAA Aviation Technology, Integration, and Operations Conference. https://doi.org/10.2514/6.2015-3288
4. Ulvi, A., Yakar, M., Yiğit, A. Y., & Kaya, Y. (2020). İHA ve Yersel Fotogrametrik Teknikler Kullanarak Aksaray Kızıl Kilisenin 3b Modelinin Ve Nokta Bulutunun Elde Edilmesi. Geomatik. https://doi.org/10.29128/geomatik.560179
5. Donateo, T., Ficarella, A., Spedicato, L., Arista, A., & Ferraro, M. (2017). A New Approach to Calculating Endurance In Electric Flight and Comparing Fuel Cells And Batteries. Applied Energy. https://doi.org/10.1016/j.apenergy.2016.11.100
6. Gur, O., & Rosen, A. (2009). Optimizing Electric Propulsion Systems for Unmanned Aerial Vehicles. Journal of Aircraft. https://doi.org/10.2514/1.41027
7. Hwang, M. H., Cha, H. R., & Jung, S. Y. (2018). Practical Endurance Estimation for Minimizing Energy Consumption of Multirotor Unmanned Aerial Vehicles. Energies, 11(9), 1–10. https://doi.org/10.3390/en11092221
8. Wannberg, M. (2012). The Quadrotor Platform - From a Military Point of View. 9 Ocak 2020 tarihinde semanticscholar: https://www.semanticscholar.org/paper/The-Quadrotor-Platform-%3A-from-a-military-point-of-Wannberg/7aae9ef8c734fbe87e063415e0210aacc37d21f3
9. Bouhoubeiny, E., Bénard, E., Bronz, M., Gavrilovic, N., & Bonnin, V. (2016). Optimal Design Of Long Endurance Mini UAVs for Atmospheric Measurement. Applied Aerodynamics Conference.

BÖLÜM5

THE EFFECT OF DIFFERENTIAL MORPHING ON THE HOVER FLIGHT IN QUADCOPTER

Lec. Oguz KOSE
Assoc. Prof. Tugrul OKTAY

THE EFFECT OF DIFFERENTIAL MORPHING ON THE HOVER FLIGHT IN QUADCOPTER

Oguz KOSE
Lec., Gumushane University, Kelkit College of Aydın Dogan

Tugrul OKTAY
Assoc. Prof., Erciyes University
Department of Aeronautical Engineering

I. INTRODUCTION

UAVs or "Unmanned Aerial Vehicles" are autonomous flying robots. Four-rotor unmanned aerial vehicles, also called quadcopters, are also included in this class. Quadcopters are designed to be used in many tasks such as search and rescue missions, border and port security, aerial photography, agriculture. Unmanned aerial vehicles, called quadcopter, have many advantages over manned aircraft such as high manoeuvrability, low cost and eliminating the risk of pilot's life.

Quadcopter control has improved tremendously over the last decade. Studies in this field have gained popularity in the literature. Studies in this area have generally focused on non-morphing quadcopters. In this study, differential morphing status of quadcopter is discussed. Differential morphing was examined for hover flights, not for all quadcopter flights. T Oktay et al. [1], they modelled a quadcopter that handled collective morphing with changing geometry. This work involved hover flight with collective morphing. In this study, the flight parameters of rise time, settling time and overshoot values do not change because they do not affect the collective flight of vertical flight. T. Oktay et al. [2], in their studies, they modelled a quadcopter with collective morphing. In

this study, they discussed only the longitudinal flight of the quadcopter. They noticed that the inertial matrix was affected in the longitudinal flight. In their simulation studies, they stated that collective morphing did not affect longitudinal flight since flight parameters did not change. T. Oktay et al. [3], in their studies, they modelled a quadcopter with collective morphing. In this study, they discussed only the lateral flight of the quadcopter. They noticed that the inertial matrix was affected in the lateral flight. In their simulation studies, they stated that collective morphing affects lateral flight since flight parameters vary. In G. Barbaraci [4], he discussed the modelling and control of a multirotor with a variable geometric arm. The arm performs morphing by increasing or decreasing its angle with the Y axis. The multirotor control system uses LQR control and PID control as well. In Gibiansky [5], the multirotor tests the multirotor designed with simulation by changing the geometry and control parameters. Evaluate simulation results and parameters obtained from experimental flights. C. Hintz et. al.[6], in his study, introduced a multirotor capable of morphing. The intended system is capable of vertical flight, in contrast to traditional multirotor. With this system, the aim is to switch vertically from narrow areas. The multirotor presents the horizontal and vertical configuration model, and the author has shown it in an animation. O Kose et al. [7], in their work they discussed on non-simultaneous morphing quadcopter. They tried all the morphing types on a quadcopter. As a result, they showed that morphing did not affect longitudinal and hover flights, but laterally.

II. QUADCOPTER DYNAMIC MODELING

Quadcopter has four rotors and propellers. Each rotor produces thrust (fi, i = 1,2,3,4). The four rotors are two pairs (1-3 and 2-4). As shown in Figure 1, one pair rotates clockwise and the other pair turns counter clockwise. This is because the counter-torque is balanced. As in Figure 1, the quadcopter makes a vertical take-off if the four rotors produce equal thrust and the thrust sum is greater than the quadcopter weight.

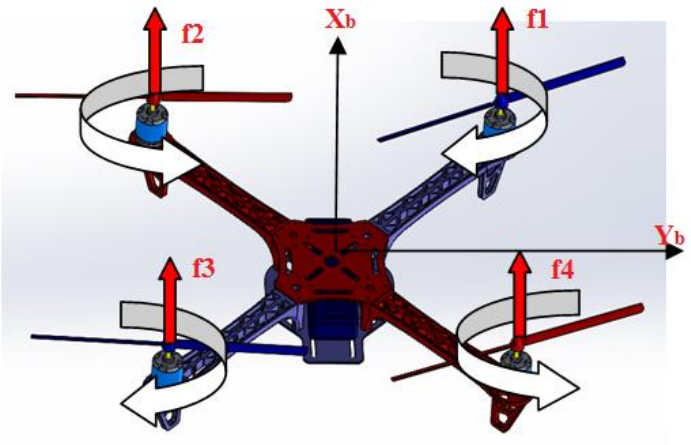


Figure 1: Quadcopter

Quadcopter motion equations have nonlinear structure. Newton-Euler approach is used for motion equations. Newton-Euler approach is used with the following assumptions[8]:

- the structure is rigid and symmetric,
- the propellers are rigid,
- the thrust and the drag are proportional to the square of speed
- ground effect is neglected.

The quadcopter motion equations consist of a total of twelve equations. These equations are the equations used for hover, longitudinal and lateral flight. From these equations x, y, z, ϕ, θ and ψ quadcopter holds the linear and angular position. u, v, w, p, q and r hold the linear and angular velocities. Quadcopter equations for hover flight are the x, z, u, w, q and θ equations.

$$\left.\begin{aligned} \dot{x} &= u \\ \dot{z} &= w \\ \dot{u} &= -g\theta \\ \dot{w} &= \frac{f_t}{m} \\ \dot{q} &= \frac{\tau_y}{I_y} \end{aligned}\right\} \quad (1)$$

$$\dot{\boldsymbol{\theta}} = \boldsymbol{q}$$

In the equations of motion I denotes the diagonal inertia matrix[9, 10].

$$\boldsymbol{I} = \begin{bmatrix} \boldsymbol{I_x} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{I_y} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \boldsymbol{I_z} \end{bmatrix} \quad (2)$$

The inputs of motion equations are propeller speeds. U1, U2, U3 and U4 are related to throttle, roll, picth and yaw respectively[11]. For vertical flight U1 and U3 input is used.

$$\left.\begin{aligned} f_t = \mathrm{U}_1 &= \mathrm{b}(\Omega_1^2 + \Omega_2^2 + \Omega_3^2 + \Omega_4^2) \\ \tau_x = \mathrm{U}_2 &= \mathrm{bl}(\Omega_3^2 - \Omega_1^2) \\ \tau_y = \mathrm{U}_3 &= \mathrm{bl}(\Omega_4^2 - \Omega_2^2) \\ \boldsymbol{\tau_z = U_4} &= \boldsymbol{d}(\Omega_2^2 + \Omega_4^2 - \Omega_1^2 - \Omega_3^2) \end{aligned}\right\} \quad (3)$$

Where l the distance between any rotor and the center of the quadcopter, b is the thrust factor and d is the drag factor and Ω is propeller speed.

Quadcopter Morphing and State Space Model

Unmanned aerial vehicles use two types of morphing. These:

- Passive morphing
- Active morphing

Passive morphing is one of the changes made in the geometry of the unmanned aerial vehicles prior to flight, while the active morphing is small physical changes aimed at optimizing the flight performance, which is performed continuously during the flight in the unmanned aerial vehicles geometry[12].

In four-rotor unmanned aerial vehicles, morphing is done by methods such as arm elongation or shortening or by changing the angles between the arm. Morphing can be used as a control element to change the flight dynamics[13].

In this study, differential morphing of quadcopter is discussed. In the case of differential morphing, the front arms are extended while the

rear arms are fixed or the front arms are fixed while the rear arms are extended. Figure 2 and Figure 3 shows morphing.

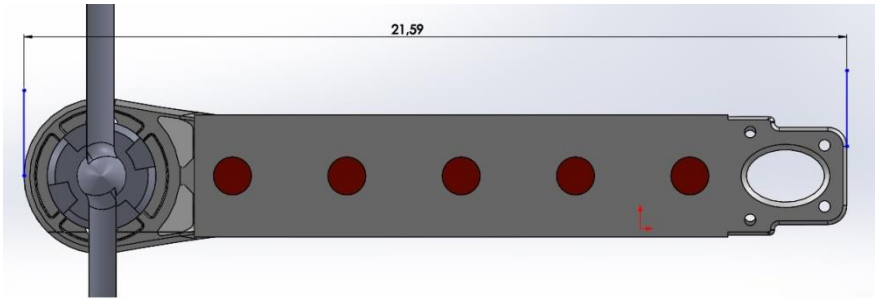


Figure 2: Normal arm(No morphing)

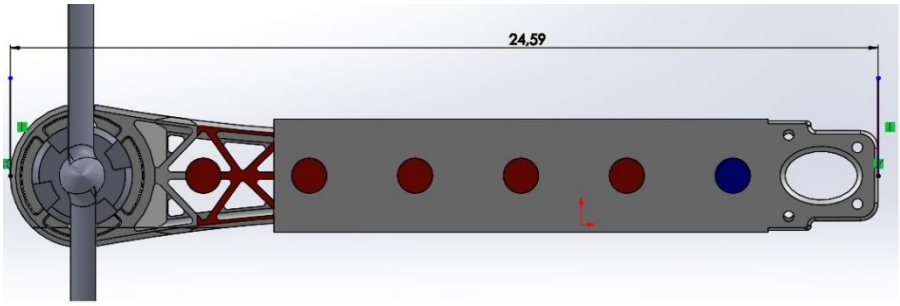


Figure 3: Differential morphing

Nowadays, it is well known that one of main advantages of the state space method is modelling of multiple-input and multiple-output control system. When the equations of a system under control is highly nonlinear it is necessary to applicate linearization[14]. The state space model is a mathematical model of a system as a set of input, output, and state variables associated with the equation from the first order. The state space model is expressed as follows:

$\dot{x} = Ax(t)+Bu(t)$

$y=Cx(t)+Du(t)$

Where x(t) state vector, u(t) control or input vector, y(t) output vector, A system vector, B input vector, C output vector and D feed forward vector.

Quadcopter state space model vectors are as follow[15].

$$\begin{bmatrix} \dot{x} \\ \dot{z} \\ \dot{u} \\ \dot{w} \\ \dot{q} \\ \dot{\theta} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -g \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ z \\ u \\ w \\ q \\ \theta \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1/m & 0 \\ 0 & 1/I_y \\ 0 & 0 \end{bmatrix} \begin{bmatrix} f_t \\ \tau_y \end{bmatrix}$$

$$y = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ z \\ u \\ w \\ q \\ \theta \end{bmatrix}$$

In the state space model, f_t refers to the throttle entry so that the quadcopter can reach the hover position. In the output vector, only the height is requested and the output z is set to 1.

Quadcopter Control System

PID is a control mechanism used in common industrial control systems. It is also widely used in quadcopter control. A PID controller calculates the difference between a set point and a desired set point in the process as an "error" value. The controller tries to reach the set point by downloading the minimum value of the error.

75% of the applications in the industry have PID applied. Karl Arstom defines this algorithm which has a wide application area as follows:

$$u(t) = K_p e(t) + K_i \int_0^t e(v)d(v) + K_d \frac{de(t)}{d(t)} \quad (4)$$

Where, K_p proportional coefficient, K_i integral coefficient and K_d is the derivative coefficient.

The control output is passed through three separate mathematical operations and is obtained by summing. System effects are as follows.

Proportional Effect (P): Effective as the output multiplied by a certain "gain" value of the error. Calculates the current error.

Integral Effect (I): The effect of the control is proportional to the sum of all the errors in the moment up to the moment the effect is

calculated. In other words, the integral effect means the sum of errors the system has made in the past.

Derivative Effect (D): It has a proportional effect on the output of the system, according to the change of the error. So it calculates the prediction of the future error.

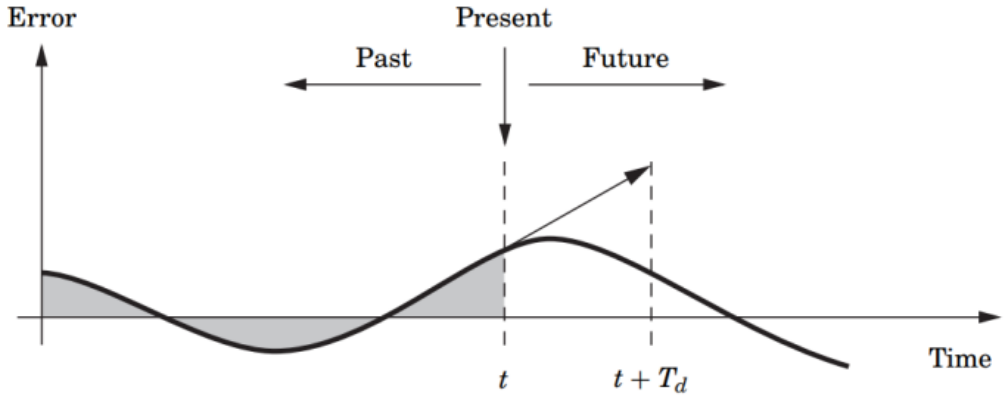


Figure 4: A PID controller takes control action based on past, present, and future

If a traditional PID structure is represented by blocks, it is as follows:

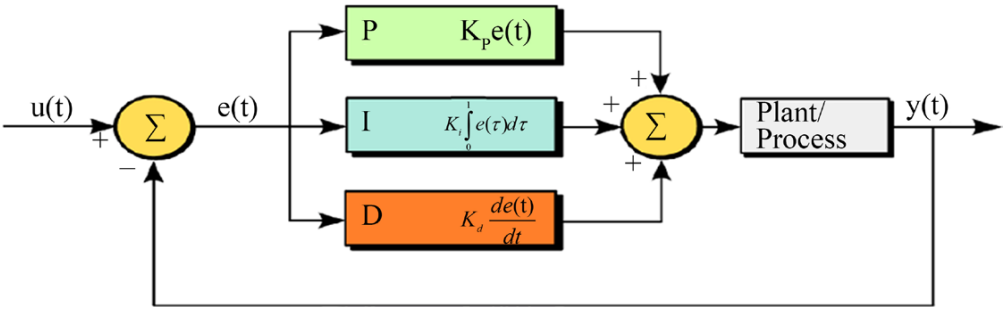


Figure 5: Traditional PID controller

Accordingly, the hover PID block is as follows:

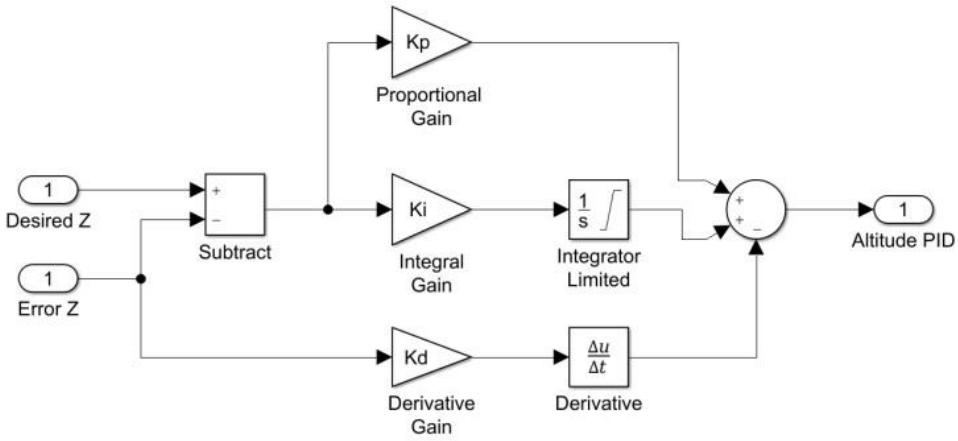


Figure 6: Hover PID block

III. RESULTS AND DISCUSSION

The top view of the quadcopter is as follows.

Figure 7: Quadcopter top view

In this case, quadcopter mass information is given in Table 1.

Table 1: Mass information (No morphing)

m= 0.59 kg

Ix=0.04085 kg*m^2
Iy=0.01629 kg*m^2
Iz=0.05607 kg*m^2

The rear arms remain fixed while the quadcopter front arms extend for differential morphing. The following figure shows differential morphing.

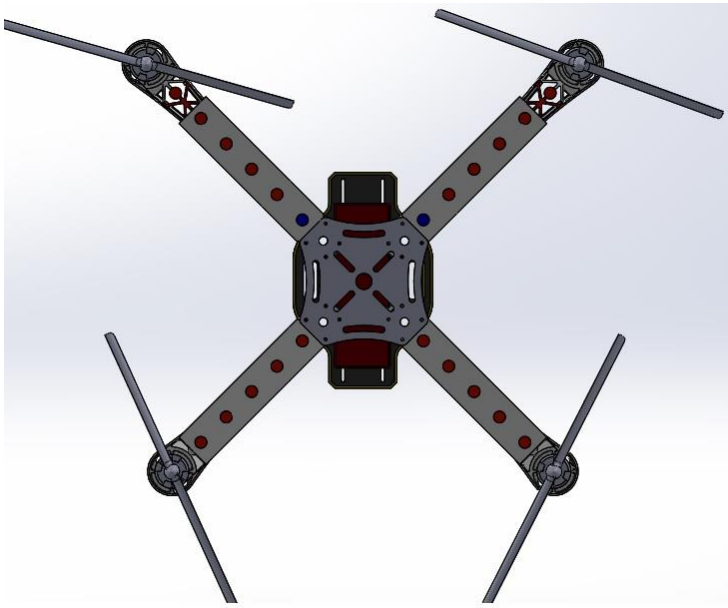


Figure 8: Differantial morphing

When differential morphing occurs, quadcopter mass information is given in the table below.

Table 2: Mass information (Differential morphing)

m= 0.59 kg
Ix=0.03859 kg*m^2
Iy=0.00668 kg*m^2
Iz=0.04418 kg*m^2

As shown in the table, differential morphing has an effect on the moment of inertia of the quadcopter. Quadcopter modelling was done in Matlab / Simulink program. The Simulink model of the hover flight is given in the following figure.

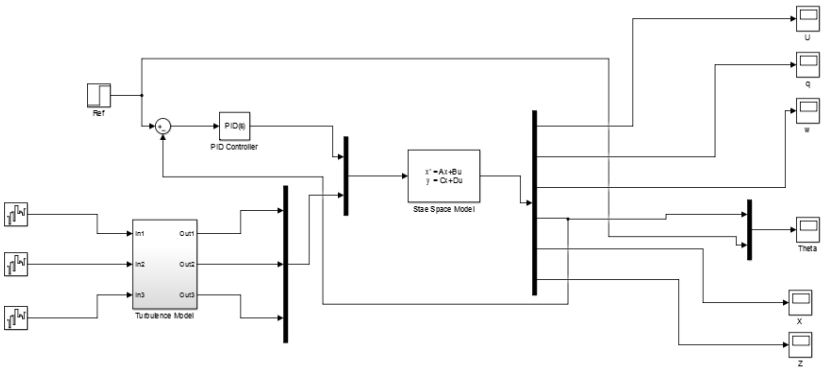


Figure 9: Simulink Model

In hover flight, the PID coefficients remain the same in both the non-morphing and morphing states. The following table shows the PID coefficients.

Table 3: PID coefficients

P	I	D
50	5	50

Hover flight simulation results are as follows.

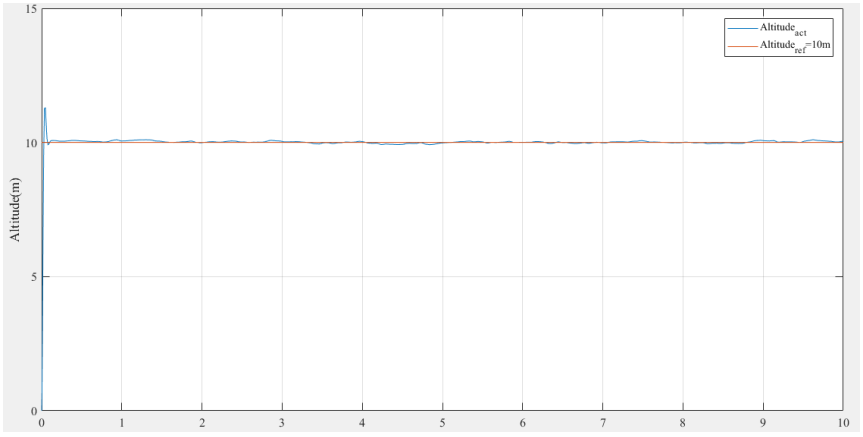


Figure 10: Hover flight(No morphing)

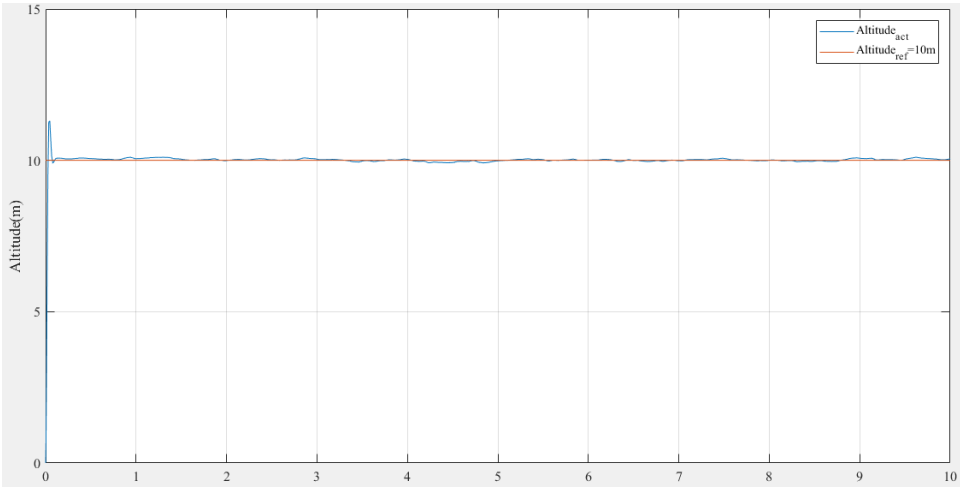


Figure 11: Hover flight (Differential morphing)

As shown in Figures 10 and 11, differential morphing did not affect quadcopter flight. It can also be seen by looking at the system characteristic.

Table 4: System characteristic

	L=21.59 cm(No morphing)	L=24.59 cm(%13 morphing)
Rise Time	0.0184 second	0.0184 second
Settling Time	0.0637 second	0.0637 second
Overshoot	1.15 %	1.15 %

IV. CONCLUSION AND FUTURE WORK

In this study, the morphing situation during quadcopter hover flight is discussed. The quadcopter dynamic model was obtained by using Newton Euler equations. The Von Karman Turbulence Model was used as an aerodynamic side effect on the quadcopter movement. The PID algorithm was used to control the quadcopter.

Design performance criteria such as rise time, settling time and overshoot have not changed in the case of morphing. Therefore, it is seen that it does not affect the morphing hover flight. If simultaneous

morphing design is performed, it is thought that it will definitely affect the result with different PID coefficients.

In the case of morphing, quadcopter has successfully followed the trajectory to follow.

References

[1] T. Oktay and O. Kose, "The Effect of Collective Morphing on the Vertical Flight in Quadcopter," in *MAS INTERNATIONAL EUROPEAN CONGRESSON MATHEMATICS, ENGINEERING, NATURAL ANDMEDICAL SCIENCES-III*, Şanlıurfa, 2019, pp. 1-10.

[2] T. Oktay and O. Kose, "The Effect of Collective Morphing on the Longitudinal Flight in Quadcopter," presented at the MAS INTERNATIONAL EUROPEAN CONGRESSON MATHEMATICS, ENGINEERING, NATURAL ANDMEDICAL SCIENCES-III, Şanlıurfa, 2019.

[3] T. Oktay and O. Kose, "The Effect of Collective Morphing on the Lateral Flight in Quadcopter," presented at the Umteb 6. Uluslararasi Mesleki ve Teknik Bilimler Kongresi, Iğdır, 2019.

[4] G. Barbaraci, "Modeling and control of a quadcopter with variable geometry arms," *Journal of Unmanned Vehicle Systems*, vol. 3, no. 2, pp. 35-57, 2015.

[5] A. Gibiansky, "Quadcopter dynamics, simulation, and control," *Andrew. gibiansky. com*, 2012.

[6] C. Hintz, C. Torno, and L. R. G. Carrillo, "Design and dynamic modeling of a rotary wing aircraft with morphing capabilities," in *2014 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2014: IEEE, pp. 492-498.

[7] O. Köse and T. Oktay, "Non Simultaneous Morphing System Desing for Quadcopters," *Avrupa Bilim ve Teknoloji Dergisi,* no. 16, pp. 577-588.

[8] A. Marks, J. F. Whidborne, and I. Yamamoto, "Control allocation for fault tolerant control of a VTOL octorotor," in *Proceedings of 2012 UKACC International Conference on Control*, 2012: IEEE, pp. 357-362.

[9] F. Sabatino, "Quadcopter control: modeling, nonlinearcontrol design, and simulation," ed, 2015.

[10] J. M. Domingue, "Quadcopter Prototype. Uneversidade Tecnica deLisboa," Dissertacio, 2009.
[11] T. Bresciani, "Modelling, identification and control of a quadcopter helicopter," *MSc Theses,* 2008.
[12] H. Çelik, T. Oktay, and İ. Türkmen, "İnsansız Küçük Bir Hava Aracının (ZANKA-I) Farklı Türbülans Ortamlarında Model Öngörülü Kontrolü Ve Gürbüzlük Testi," *Journal of Aeronautics & Space Technologies/Havacilik ve Uzay Teknolojileri Dergisi,* vol. 9, no. 1, 2016.
[13] V. Prisacariu, V. Sandru, and C. Rău, "Introduction morphing technology in unmanned aircraft vehicles (UAV)," in *International Conference of Scientific Paper, AFASES,* 2011.
[14] T. Tengis and A. Batmunkh, "State feedback control simulation of Quadcopter model," in *2016 11th International Forum on Strategic Technology (IFOST),* 2016: IEEE, pp. 553-557.
[15] O. Kose and T. Oktay, "Optimal Tunning of PID Controller For Forward Flight of Research Based Quadcopter," presented at the 2. Uluslararası Multidisipliner Çalışmaları Kongresi, Adana, 2018.

BÖLÜM6

BLOKZİNCİRDE İMZALAMA ALGORİTMALARI

YL. Öğrencisi Roda KIZIL
Dr. Öğr. Üyesi Süleyman KARDAŞ

BLOKZİNCİRDE İMZALAMA ALGORİTMALARI

THE SIGNING ALGORITHMS IN BLOCKCHAIN

Roda KIZIL
Yüksek Lisans Öğrencisi, Batman Üniversitesi Fen Bilimleri Enstitüsü Elektrik elektronik Mühendisliği Anabilim Dalı, (Sorumlu Yazar)

Süleyman KARDAŞ
Dr. Öğr. Üyesi, Batman Üniversitesi Mühendislik ve Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü

GİRİŞ

Türkçe anlamı Blok-Zinciri olan Blokzincir, ilk kez dijital para Bitcoinin arkasındaki teknoloji olarak ortaya çıkmıştır [6]. Blokzincir teknolojisi hayatımıza Satoshi Nakamoto takma isimli kişi veya kişilerin Ekim 2008'de yayınladığı "Bitcoin: Eşten Eşe Elektronik Ödeme Sistemi" makalesi ile ortaya çıkmıştır. Birkaç insanın para transferi işlemini kimseye gerek kalmadan daha doğrusu merkezi bir yere bağlı kalmadan gerçekleştirme isteği Blokzincir teknolojisinin ortaya çıkmasına neden olmuştur [19].

Blokzinciri, merkezi bir yerden yönetilemeyen, ağda bulunan tüm üyelerin (düğümlerin) birbirlerine güven duymalarına gerek kalmadan içerisindeki verilerin herhangi bir saldırgan tarafından değiştirilemeyeceği, herkese açık, şeffaf, dağıtık, sıralı aynı zamanda zaman damgalı verilerin tümünü içinde barındıran bir kayıt defteri olarak tanımlanmaktadır. Paranın güvenliğini bankalardan alan Bokzinciri bu teknolojik yaklaşımları Kriptografik zor matematiksel problemlere devretmektedir. Blokzincirin etki alanlarının kripto paraların çok daha ötesinde olduğu ve pek çok sektörde uygulanabilir olduğu, günümüzde yapılan birçok çalışmayla desteklenmektedir [6]. Blokzincir ile tüm verilerin kayıt altına alınması ve transfer işleminin gerçekleştirilebilir olması Blokzincir teknolojisinin önemini daha da artırmıştır [18].

Blokzincir teknolojisinde bu işlemlerin imzalanmasında eliptik eğri kripto sistemi kullanılarak ECDSA (Eliptik Eğri Tabanlı Dijital İmza Algoritması) ve EDDSA (Edwards eğri dijital imza algoritması) imzalama

algoritmaları kullanılır. Bu makaledeki amacımız Blokzincirde kullanılan bu imzalama yöntemlerinin neler olduğunu, aralarındaki benzer noktaları ve farklarını ele alarak, birbirlerine olan üstünlük ve güvenlikleri açısından değerlendirilip karşılaştırılmasının verilmesidir.
Makalenin ilk bölümünde eliptik eğri kripto sistemi (EEC) ele alınmıştır. İkinci bölümde ECDSA (Eliptik Eğri Tabanlı Dijital İmza Algoritması) imzalama algoritmasına değinilip, imza oluşturma ve imza doğrulamanın nasıl yapıldığı anlatılmıştır. Üçüncü bölümde EDDSA (Edwards eğri dijital imza algoritması) imzalama algoritması ele alınıp alt parametrelerinden bahsedilmiştir. Son bölümde ise ECDSA ve EDDSA 'nın aralarındaki farklar ele alınarak birbirlerine olan üstünlük ve güvenlikleri açısından değerlendirilip karşılaştırılması verilmiştir.

ELİPTİK EĞRİ KRİPTOSİSTEMİ

RSA (Rivest, Shamir, ve Adleman) kriptosistemine alternatif olarak Neal Koblitz [13] ve Victor Miller [17], eliptik eğri tabanlı açık anahtar kripto sistemini (EEC) 1985 yılında öne sürdüler [6]. EEC algoritmasının en büyük özelliği diğer açık anahtar şifreleme sistemlerinin güvenliğini daha düşük anahtar uzunluğu ile sağlayabilmesidir [28].
EEC 'nin güvenilirliğini modüler ayrık logaritma problemi (MALP) sağlar [27]. Örneğin, 160-bitlik bir EEC anahtarının güvenlik seviyesi ile 1536-bitlik bir RSA anahtarının güvenlik seviyesi eşdeğerdir. Ayrıca bu eşdeğer güvenlik seviyesinde EEC şifrelemede RSA 'ya göre daha hızlıdır [20]. EEC gerekli olan güvenlik seviyesini daha küçük anahtar boyutuyla sağlayabilmektedir. Bu özellikleri ile EEC, RSA' ya göre daha az maliyetli olup daha az bellek tüketiminde bulunmaktadır [10]. EEC ile RSA anahtar boyutları ve güvenlik seviyeleri Tablo'1 de verilmektedir.

Tablo 1. *ECC ile diğer algoritmaların anahtar uzunluklarının karşılaştırılması ([27],[28])*

Güvenlik Seviyesi (Bits)	**DSA**	**RSA**	**ECC**
80	1024	1024	160
112	2048	2048	224
128	3072	3072	256
192	7680	7680	384
256	15360	15360	512

1024 bit anahtar uzunluğuna sahip olan RSA ile sağlanan güvenlik, EEC'nin 160-bit anahtar değeri kullanılarak sağlanabilmektedir [27]. EEC' de güvenlik bir eliptik eğride tanımlı noktalar üstünde kurulu ayrık logaritma problemine dayandırılmıştır [2].

ELİPTİK EĞRİ (ELLIPTIC CURVE)

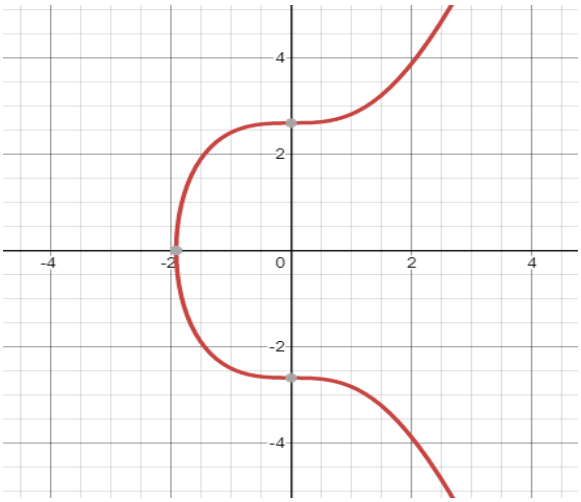
Bir eliptik eğri, kendisini tanımlayan polinomdaki denkliği sağlayan (x,y) noktalarından oluşur. Eliptik eğri genel denklemi;

$$y^2 = x^3 + a * x + b \ (mod\ p)\ ,\quad x, y\ a, b \in R$$

olarak verilmektedir.

Eğer (x, y) yukarıdaki eşitliği sağlıyorsa P (x, y), eliptik eğri üstünde bir nokta olduğu kabul edilir [2]. $y^2 = x^3 + a * x + b\ (mod\ p)$ denklemindeki a ve b sayıları gerçel sayılardır ve $x^3 + a * x + b$ denkleminin çoklu kökü olmaması için $\Delta = -16(4a^3 + 27b^2) \neq 0$ denkleminin sağlanması gerekmektedir. Eğer bu koşulları sağlıyorsa $y^2 = x^3 + a * x + b\ (mod\ p)$ eliptik eğri imzalama algoritmalarında kullanılmaktadır. Böylece eliptik eğri tekil olmaz ve sonlu sayıda (x, y) nokta çifti ile çözümlenebilir [15]. Eliptik eğriler, gerçek, tamsayı ya da kompleks cisimlerden herhangi birisi üstünde tanımlanabilir. Ancak bir kripto sistem için kullanıldığında, tamsayı ve asal bir mod değerine göre işlemlerin yapıldığı sonlu cisimler tercih edilir. Bu noktada dikkat edilmesi gereken özellik, kullanılan asal sayının büyüklüğü ve eliptik eğriyi tanımlayan polinom ile, bu cisim üstünde sağlanan noktaların sayısının ne denli çok olduğudur. Bir sonlu cisim, toplama ve çarpma gibi aritmetik işlemlerde sonlu sayıda eleman içerir ve bilgisayar ortamlarında işlemlerin kolaylaştırılması ve hızlandırılması amacıyla, ikili sonlu cisimler (F_{2^m}) kriptografik uygulamalar üzerindeki eliptik eğri grupları özellikle tercih edilir [2].

Denklemi $y^2 = x^3 + 7$ olarak verilmiş eliptik eğri grafiği şu şekilde verilmektedir (Bknz.
Şekil **1**).

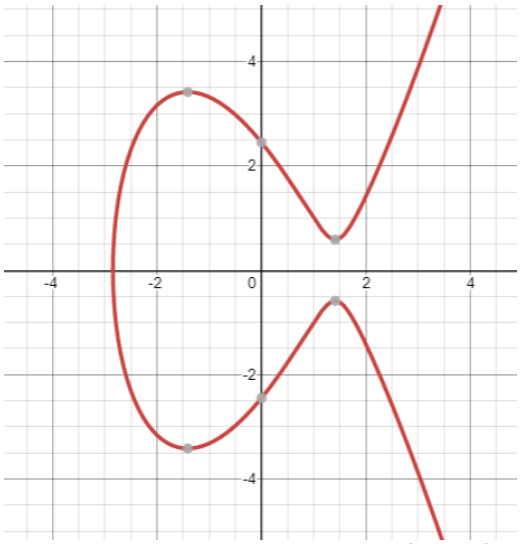


***Şekil 1**. Eliptik Eğri Grafiği* ($y^2 = x^3 + 7$)

ELİPTİK EĞRİ ÜZERİNDE ARİTMETİK İŞLEMLER

Herhangi bir (x, y) noktası eliptik eğri üzerinde olması (x, y) noktasının $y^2 = x^3 + a * x + b\ (mod\ p)$ denklemindeki eşitliği sağlaması ile anlaşılmaktadır. Eliptik eğri sistemlerinde, paralel iki doğrunun sonsuz uzaydaki kesiştiği noktaya O (Point at Infinity) adı verilmektedir.

$P(x_p, y_p)$, $Q(x_q, y_q)$, ve $R(x_r, y_r)$ $P = Q$ olmak üzere; $x_p = x_q$ olduğu durumda P ve Q noktaları x eksenine göre simetrik olacağından dolayı doğru eğriye dik olacaktır. Bu durumda doğru eğriyi üçüncü bir noktada kesemez. Bu nedenle bu iki nokta eğriyi sonsuzda 'O' noktasında kestiği için P+Q=O olur [1, 29]. $x_p = x_q$ ve $y_p \neq y_q$ ise $P = -Q$ ve $m_{p,q} = \infty$ olacağından P ve Q noktalarının birleştirecek olan doğru y eksenine paralel olacağından bu doğru eğriyi sonsuzdaki 0 noktasında keser ve böylelikle $P + Q = O$ sonucuna ulaşılır [29]. Eliptik eğri üzerindeki noktaların toplanması durumunda geometrik yöntemler kullanıldığı gibi matematiksel formüllerde kullanılır (Bknz. Şekil 2).



***Şekil 2**. Nokta ekleme sonsuz durumu ($y^2 = x^3 - 6x + 6$)*

İki boyutlu/üç boyutlu

Eliptik eğriler, 3. dereceden fonksiyon kullanılarak tanımlanır. Polinom, birbirini dik kesen eksenlerin oluşturduğu iki boyutlu düzlem ya da üç boyutlu uzay olan, kartezyen (Euclidean) koordinat sistemi üzerinde eliptik eğriyi tanımlar. Herhangi bir nesne üzerinde bir noktayı tanımlamak için gereksinim duyulan sayısal değerlerin adedi, koordinat sisteminin boyutunu belirler. Örneğin, bir dörtgen iki boyutluyken, küp üç boyutludur. Tanım genelleştirildiğinde; *n* boyutlu bir koordinat sistemi, $R^n = (x_1, x_2, \dots, x_n)$ gibi *n* adet gerçek sayı ile gösterilebilir.

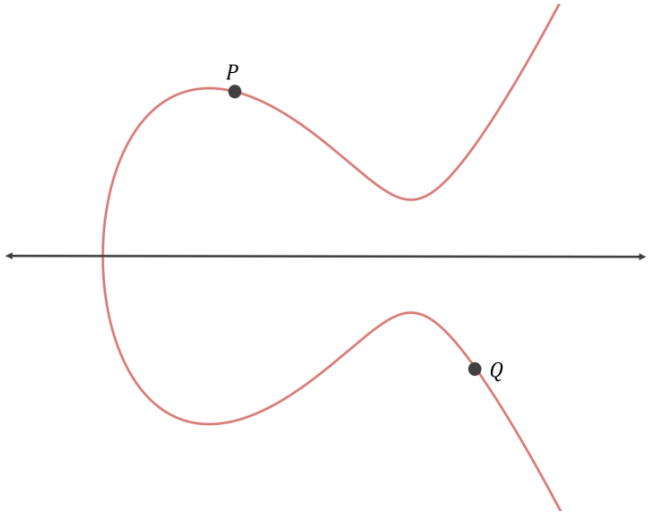
Eliptik eğri (EE) aritmetiği, iki ve üç boyutlu kartezyen koordinat sistemleri olan;

- İki boyutlu
  - Afine (Affine)
- Üç boyutlu
  - Projektif (Projective)
  - Jacobian
    - Modified Jacobian
    - Chudnovsky Jacobian

Farklı koordinat sistemleri arasında geçişi tanımlayan eşleşme fonksiyonları kullanılarak, aynı eliptik eğri için gerekli aritmetik işlemler farklı koordinat sistemlerinde yapılabilir [3].

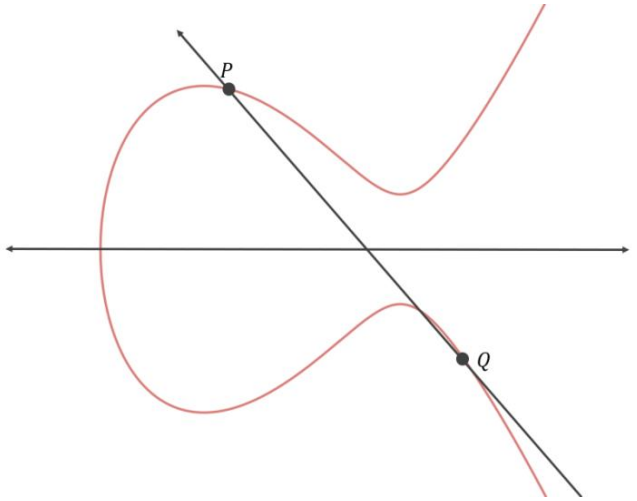
FARKLI İKİ NOKTANIN TOPLANMASI

Eğri üzerinde iki nokta (P ve Q) ile tanımlanan bir doğrunun eğriyi başka noktada üçüncü kez kesiştiği gerçeğinden yararlanmaktadır. P ve Q'yu birbirine eklemek demek, üçüncü nokta R'nin x ekseninde simetrisini almak demektir.
Eliptik bir eğri üzerine iki nokta birlikte eklemek için, önce bu iki noktadan geçen çizgi bulunur. Bulunan çizginin üçüncü noktadaki eğriyi kestiği yer belirlenir. Üçüncü nokta x ekseni boyunca yansıtılır, x eksenine göre simetriği alınır (yani, y koordinatı -1 ile çarpılır) ve bu noktadan elde edilen nokta, ilk iki noktanın (P ve Q) birbirine eklenerek üçüncü noktanın (R)'nin elde edilmesidir.
Bunun bir örneğine bakalım;
P ve Q noktalarının eğri üzerinde yerleri belirlenir.



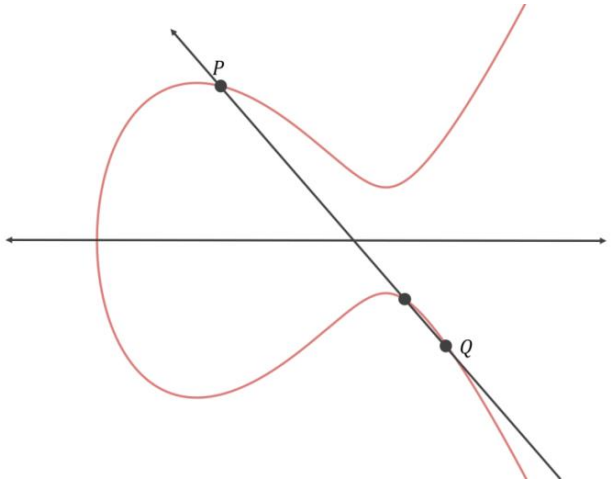
***Şekil 3**. Eliptik Eğri Grafiği: P ve Q noktası*

İlk önce, iki noktadan geçen çizgi bulunur (Bknz. Şekil 3 ve Şekil 4),



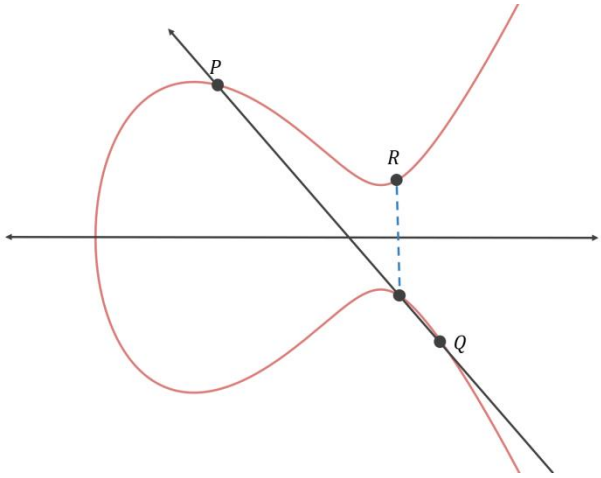
Şekil 4. *Eliptik Eğri Grafiği: P ve Q noktalarından geçen doğru*

Doğru ile eğrinin kesiştiği nokta belirlenir.(Bknz. Şekil 5),



Şekil 5. *P ve Q noktalarının eğri ile kesiştiği nokta*

Sonra bu nokta x ekseni boyunca yansıtılır. X koordinatına göre simetriği alınır.



Şekil 6. *P ve Q noktalarının birbirine eklenmesi (P+Q=R)*

Bu nedenle $\boldsymbol{P + Q = R}$ olur.

Toplama Algoritması $\boldsymbol{P = (x_1, y_1)}$, $\boldsymbol{Q = (x_2, y_2)}$ olarak verildiğinde;
$\boldsymbol{R = P + Q = (x_3, y_3)}$:

$$\boldsymbol{Eğim(s) = \frac{y_2 - y_1}{x_2 - x_1}}$$

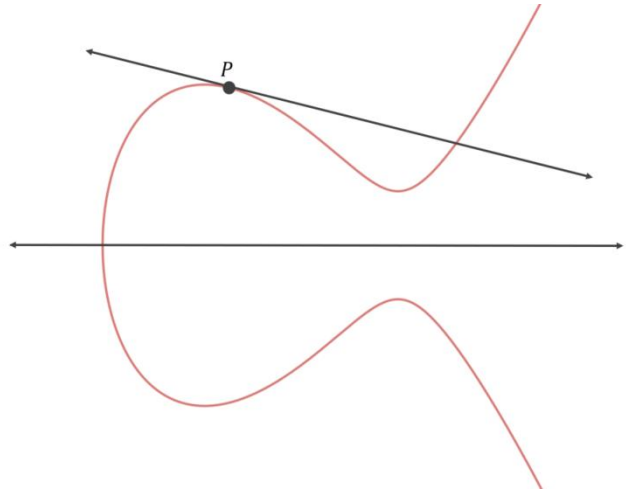
$$\boldsymbol{x_3 = s^2 - x_1 - x_2}$$

$$\boldsymbol{y_3 = s(x_1 - x_3) - y_1}$$

AYNI İKİ NOKTANIN TOPLANMASI (DOUBLING)

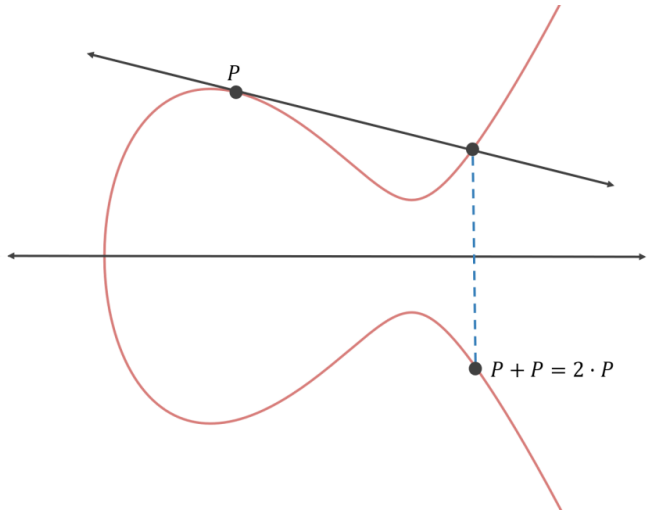
Eğri üzerindeki noktanın (P) tanjantının başka noktada (R) ikinci kez kestiği gerçeğinden yararlanmaktadır. P noktasının ikiye katlamak demek tanjantının kestiği noktanın x ekseninde simetrisini almak demektir.

Örneğin, P temel noktası ile aşağıdaki eğriye sahip olduğumuzu varsayalım: Başlangıçta, P veya 1P var. Bu tür sonsuz sınırların olduğu özel durumda, teğet çizgi tercih edilir.



Şekil 7. *P noktasının eğriye teğeti*

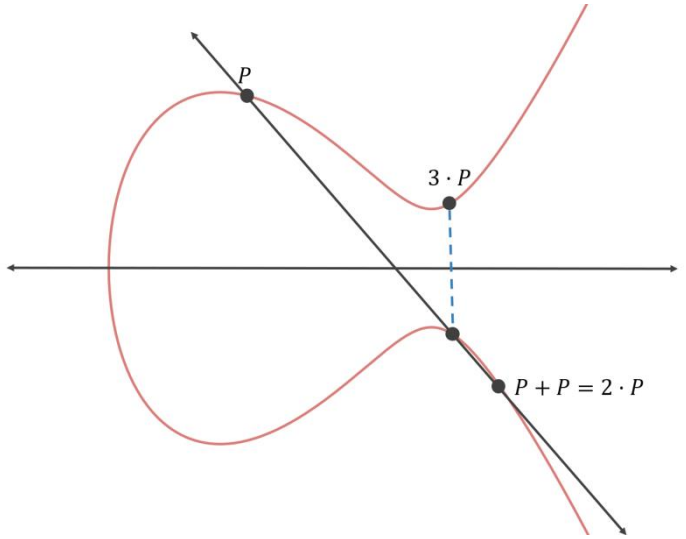
Şimdi bu çizginin kesiştiği ve x ekseni boyunca yansıttığı "üçüncü" nokta bulunur.



Şekil 8. *İki P noktasının birbirine eklenmesi(P+P=2P)*

Böylece P kendi kendine eklenir veya P + P, 2 • P'ye eşittir.

2P'ye tekrar P eklersek, (2P+P=3P) den yola çıkarak buluruz. Öncelikle P ve 2P noktalarını grafikte belirleyip bu noktalardan geçecek şekilde bir doğru çekilir. Doğru ile eğrinin kesiştiği nokta belirlenir ve x koordinatına göre simetriği alınır.



Şekil 9. *P ve 2P noktalarının birbirlerine eklenmesi(P+2P=3P)*

Böylelikle $P + 2P = 3P$ noktası bulundu. $4P,\ 5P, \dots, nP$ noktalarını hesaplamak için aynı yöntemle devam edilerek bulunur. Bu şekilde devam edilip istenilen nP değeri bu yöntemle bulunabilir.

Şekil 1'deki verilen $y^2 = x^3 + 7\ (mod\ 23)$ denklemi üzerinde bulunan $P_1 = (1{,}10)$ noktası verilsin. $P_2 = P + P = (X_2, Y_2)$ noktasını bulalım;

$$y^2 = x^3 + a * x + b\ (mod\ p)\ ,\quad x, y\ a, b \in R$$

$a = 0, b = 7;$

$$Eğim(s) = \frac{3{x_1}^2 + a}{2y_1}$$

$$x_2 = s^2 - 2x_1$$

$$y_2 = s(x_1 - x_2) - y_1$$

Formülleri kullanılarak 2P bulunur. Tablo 2'de tüm 23P değerleri bulunmuştur (Tablo2'e bknz.)

***Tablo 2**. Nokta ekleme, skaler nokta çarpımsal değeri*

1P=[1,10]	7P=[8,6]	13P=[16,3]	19P= [19,14]
2P =[22,11]	8P=[4,18]	14P=[10,8]	20P= [11,21]
3P=[6,4]	9P=[20,16]	15P=[20,7]	21P= [6,19]
4P=[11,2]	10P=[10,15]	16P=[4,5]	22P= [22,12]
5P=[19,9]	11P=[16,20]	17P=[8,17]	23P= [1,13]
6P=[15,1]	12P=[9,0]	18P=[15,22]	

SKALER ÇARPMADA HIZLANDIRMA

Eliptik eğri üzerindeki herhangi bir noktanın k skaler sayısı ile çarpılma işlemi eliptik eğri üzerindeki en temel işlemlerden biridir. Q ve P eliptik eğri üzerinde seçilen iki nokta ve k bir tamsayı olmak üzere skaler çarpma işlemi aşağıdaki gibi olur.

$$Q = k.P$$
$$Q = P + P + \cdots + P$$

Buradaki k sayısı küçük olabileceği gibi büyük bir değerde olabilir ve k değerinin büyük olması durumunda sistemin hem maliyetini hem de karmaşıklığını artıracağından dolayı hem maliyeti hem de karmaşıklığı en aza indirmek ve işlemin en hızlı şekilde gerçekleşmesini sağlamak için birçok algoritma geliştirilmiştir. k değerinin çok büyük olduğu durumunda $Q = k.P$ işlemi hem çok uzun sürüp hem de çok fazla işlem gerektirmektedir. Bu durumda $Q = k.P$ çarpımının yapılması için ikile ve topla algoritması kullanarak işlem gerçekleştirilebilir. [16].

10 • P'yi hesaplamak için 9 nokta ekleme işlemi gerektirir. Fakat ikile ve topla yöntemini kullanarak Sadece dört adımda $10 \bullet P$ hesaplanarak 4 adıma indirgenebilir. Bunun nedeni, aşağıdaki özelliğin nokta ekleme için geçerli olmasıdır:

$$n \bullet P + r \bullet P = (n + r) \bullet P$$

Örneğin:

$$4 \bullet P + 6 \bullet P = (4 + 6) \bullet P = 10 \bullet P$$

Böylece, $10 \bullet P$ ' yi hesaplamanın hızlı yolu şöyledir:

$P + P = 2 \bullet P$
$2 \bullet P + 2 \bullet P = 4 \bullet P$
$4 \bullet P + 4 \bullet P = 8 \bullet P$
$2 \bullet P + 8 \bullet P = 10 \bullet P$

bu sadece dört nokta ekleme işlemi gerektirir.
İkile ve Topla Algoritması aşağıdaki gibi algoritma kullanılarak uygulanır.

İkile ve Topla Algoritması

Giriş: $k_{n-1} = 1$ olmak üzere $K = k_{n-1}2^{n-1} + k_{n-1}2^{n-2} + \cdots + k_1 2 + k_0$ ve $P = (x, y)$
Çıkış: $Q = kP = (x', y')$

1. $Q < -P$
2. for i from $n - 2$ downto () do
3. $Q < -2Q$
4. İf $k_1 = 1$ then
5. $Q = Q + P$
6. end if
7. end for

[26].

100• P'nin hesaplanması bu algoritmayla şöyledir:

$100_2 = 1100100 = 64P + 32P + 4P$;
$P + P = 2 \bullet P$
$2 \bullet P + 2 \bullet P = 4 \bullet P$
$4 \bullet P + 4 \bullet P = 8 \bullet P$
$8 \bullet P + 8 \bullet P = 16 \bullet P$
$16 \bullet P + 16 \bullet P = 32 \bullet P$
$32 \bullet P + 32 \bullet P = 64 \bullet P$

Böylelikle 100P hızlı bir şekilde bulunur.

Skaler çarpma işlemi, nokta çiftleme ve nokta toplama işlemleri kullanılarak yapılmaktadır. Verilen bu algoritmanın kullanılmasında

oluşan sonuç genelleştirilirse; $l\ bit$ uzunluklu k değeri için $(l-1)$ ikile işlemi, $(l-1)/2$ toplama işlemi ile skaler çarpma tamamlanır. Toplam karmaşıklık ise $\frac{3}{2}(l-1)$ 'dir [26].

ECDSA (ELİPTİK EĞRİ DİJİTAL İMZA ALGORİTMASI)

Eliptik eğri dijital imza algoritması (ECDSA), dijital imza algoritması (DSA) 'nın eliptik eğri tabanlı bir imzalama algoritmasıdır.[11,12]. 1992 yılında hazırlanmış ve 1999 yılında ANSI (Amerika Ulusal Standartlar Enstitüsü) [4] , 2000 yılında ise IEEE (Elektrik ve Elektronik Mühendisleri Enstitüsü) [8] ve ISO (Uluslararası Standardizasyon Teşkilatı) [9] tarafından standart olarak kabul edilmiştir [24].

Bitcoin, imzalama ve şifreleme anahtarlarının üretiminde ECC kullanır. Ek olarak, RSA 'ya kıyasla ECC, şu anda bazı uygulamalar için bir avantaj olabilen yeni şifreleme protokollerinin oluşturulmasına izin veren eşleşmelerin hesaplanmasına izin vermektedir. NIST [5] ve Certicom eliptik eğri algoritmik özelliklerinin çoğunun patentlendikleri bilinmektedir. Her ikisi de a, b ve p parametrelerini kullanan Weierstrass tabanlı eğrilerin kullanımını önermektedir. Özellikle, Secp256r1 ve secp256k1 eğrilerini kullanan Weierstrass tabanlı eğrileri kullanmayı önermektedir. Bu makalede, blokzincir teknolojsinde en çok kullanılan secp256r1 eğrisi ve Koblitz Secp256k1 eğrisi ele alınmıştır [7].

ECDSA PARAMETRELERİ

NIST eğrileri: secp521r1, secp384r1, secp256r1, secp224r1, secp192r1
Koblitz eğrileri: secp256k1, secp224k1, secp192k1
FIPS186-4'ün P-192, secp192r1 olarak, P-224 secp224r1 olarak, P-256 secp256r1 olarak, P-384 secp224r1 olarak ve P-521 secp521r1 olarak anlamlandırılır.

Secp256k1 ve secp256r1 Parametresi

Secp256k1, Bitcoinde kullanılan eğrinin ECDSA parametrelerini belirtir ve Verimlilik Şifreleme Standartları (SEC) ile tanımlanır [25]. SECG adını kullanan bir grup tarafından yayınlanan, SEC2 adlı bir standarttan secp256k1 olarak adlandırılır. Secp256k1 adını parçalar şeklinde açıklarsak: Sec standart anlamını taşır, p, eliptik eğri koordinatları üzerinde bir asal alan olduğu anlamına gelir, 256 sayısı parametrenin 256

bit uzunluğunda olduğu, k ise Koblitz eğrisi üzerinde bir varyant olduğu anlamına gelir ve 1 bu türün standarttın ilk eğrisidir. Koblitz eğrileri, hesaplamaları hızlandırmak için kullanılabilecek bazı iç yapıya sahip özel bir eliptik eğri türüdür. Secp256k1, Bitcoin popüler olmadan önce neredeyse hiç kullanılmamıştı, ancak birçok özelliği nedeniyle popülerlik kazanmaktadır. Bu, Secp256r1 eğrisi gibi NIST tarafından değil Certicom (Kanadalı bir şirket) tarafından üretildi [7]. Secp256r1 eğrisi rastgele bir yapıya sahip iken secp256k1 eğrisi rastgele olmayan bir yapıya sahiptir. Secp256k1 eğrisinde hesaplamalar verimli olup hızı diğer eğrilere göre %30 daha hızlıdır.

Çoğu standart, asal alanları kullanırken rastgele eğri denilen şeyi kullanır. SEC2 ayrıca rasgele eğriler içerir ve secp256k1'den sonraki sekans secp256r1 olarak adlandırılır. Bu eğri, secp256r1, ABD hükümeti de dahil olmak üzere P-256 olarak adlandırılan yaygın bir şekilde standartlaştırılmış ve kullanılmıştır.

Bir Koblitz eğrisi Secp256k1 ile ilişkili F_p üzerindeki alanın eliptik eğri parametreleri, sonlu alanın $T = (p, a, b, G, n, h)$ ile tanımlandığı, Secp256k1 parametresi, $Tablo$ 3 [25] 'da gösterilmiştir [7]. Secp256k1'in eğrisinin denklemi; $y^2 = x^3 + 7$ olarak verilmiştir (Bknz.

Şekil **1**).

***Tablo 3**- Secp256k1 parametresi [25]*

Parametre	**Değer**
P	$2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ Ffffffffffffffffffffffffffffffffffffffffffffffffffffffefffffc2e
A	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
B	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007
G	04 79be667e f9dcbbac 55a06295 ce870b07 029bfcdb 2dce28d9 59f2815b 16f81798 483ada77 26a3c465 5da4fbfc 0e1108a8 fd17b448 a6855419 9c47d08f fb10d4b8
N	fffffffffffffffffffffffffffffffe baaedce6 af48a03b bfd25e8c d0364141

H	1

Tablo 4'e bakıldığında Secp256r1 eğrisinin, secp256k1 eğrisinden hem daha güvenilir hem de daha maliyetli olduğu görülmektedir.

Tablo 4*- secp256r1 ve secp256k1 parametrelerinin karşılaştırılması*

Eğri	**Secp256r1**	**Secp256k1**
Güvenlik	$2\sqrt{\frac{\pi nsec256r1}{4}} = 127.83$	$2\sqrt{\frac{\pi nsec256k1}{2}} = 127.03$
Otomorfizm Sırası	2	6
"A" parametreleri	3	a = 0 eğrinin denkleminin ekseni terimi her zaman sıfırdır
Maliyet	$2^{120,3}$	$2^{109,5}$

Sayısal imza; sanal ortamda taraflar arasında yürütülen işlemlerde, elle atılan imzanın yerini alır. Sayısal imza uygulamasıyla; kimlik denetimi, mesajın özgünlük ve doğruluk/bütünlük denetimi ile, inkar edilemezlik sağlanır. Başlıca dört algoritmadan oluşur.

1. Alan parametrelerini belirleyen algoritma; bu algoritmayla alan parametreleri belirlenerek, iletişim ortamını kullanacak herkese duyurulur.
2. Anahtar oluşturma algoritması
3. İmza oluşturma algoritması
4. İmza doğrulaması yapan algoritma [14].

ECDSA ile ilgili bilinmesi gereken birkaç kavramı ele alalım:

Gizli anahtar (Private key): Gizli anahtar sadece anahtarı oluşturan kişi tarafından bilinen anahtardır. Özel anahtarlar 256-bit sayı formatında oluşturulur.
Açık anahtar (Public key): Gizli anahtara karşılık gelen, fakat gizli tutulmasına gerek kalmayan herkese açık bir anahtardır.

Açık anahtar ile şifrelenen veri Gizli anahtar ile, Gizli anahtar ile şifrelenen veri ise Açık anahtar ile deşifre edilebilir. Adlarından da anlaşılacağı gibi Gizli anahtar kişiye özel bir anahtar, Açık anahtar ise herkese açık bir anahtardır. İletişime geçilmek istenen kişinin Açık anahtarı ile şifrelenen veri sadece ilgili kişinin Gizli anahtarı ile deşifre edilebileceği için güvenli bir şekilde göndermek istenen kişiye iletilebilir.

1. Alan parametrelerini belirleyen algoritma

ECDSA'da kullanılan eliptik eğri algoritmaları ya asal tek sayılar (Z_p) ya da sonlu alanlar ($GF(2^m)$) üzerine uygulanır. Girdi olarak kullanılan veriler, SHA-1 algoritması ile özeti alındıktan sonra 160 bit olarak işlenir. ECDSA'ya ait parametreler ve açıklamalarına aşağıda yer verilmiştir [4,21].

1) $q; p$ veya 2^m için alan uzunluğunu belirtir,
2) $a, b \in$ Zp veya $a, b \in GF(2^m)$ olmak üzere;
$\boldsymbol{Z_p}$ ve $\boldsymbol{p > 3}$ için: $\boldsymbol{y^3 = x^2 + ax + b}$
$\boldsymbol{GF(2^m)}$ ve $\boldsymbol{p = 2^m}$ için $\boldsymbol{y^2 + xy = x^3 + ax^2 + b}$
3) $\boldsymbol{G = x(G), y(G)}$
ECDSA algoritması kullanılarak anahtar oluşturma, imzalama ve imza doğrulama aşamaları aşağıda yer verilmiştir [4, 21].

2. Anahtar oluşturma
A kullanıcısı için anahtar çifti, ortam için tanımlanan eliptik eğri tabanlı alan parametreleri
$\boldsymbol{D = (q, FR, a, b, G, n, h)}$ kullanılarak oluşturulur. Anahtar çiftini oluşturacak algoritma işletilmeden önce *A* kullanıcısı alan parametrelerinin geçerliliğini ve doğruluğunu kontrol etmelidir. *A* kullanıcısı anahtar çiftini oluşturmak için:
a. $\boldsymbol{[1, n-1]}$ aralığında rastgele bir d sayısı seçilir.
b. $\boldsymbol{Q = x(Q), y(Q)}$ kullanılarak $\boldsymbol{Q = dP}$ hesaplanır,
c. *Açık* anahtarı $\boldsymbol{Q}$, gizli anahtarı $\boldsymbol{d}$ 'dir. [3]

3. İmza Oluşturma
m mesajının imzalanmasında, *A* kullanıcısı $\boldsymbol{D = (q, FR, a, b, G, n, h)}$ alan parametreleri ve anahtar çifti $\boldsymbol{(d, Q)}$ bilgilerini kullanarak:

1. $\boldsymbol{1 \leq k \leq n-1}$ aralığında rastgele bir k değeri seçilir.
2. $\boldsymbol{\bar{m} = SHA1(m)}$ hesaplanır

3. $(\boldsymbol{x1}, \boldsymbol{y1}) = \boldsymbol{kG}$ hesaplanır ve $\boldsymbol{x_1}$ tamsayı değerine çevrilerek $\overline{\boldsymbol{x_1}}$ bulunur [3].
4. $\boldsymbol{r} = \overline{\boldsymbol{x_1}} \boldsymbol{mod}(\boldsymbol{n})$ hesaplanır, $\boldsymbol{r} = \boldsymbol{0}$ ise 1. adıma geri gidilir.
5. $\boldsymbol{s} = \boldsymbol{k^{-1}}(\overline{\boldsymbol{m}} + \boldsymbol{dr})\ \boldsymbol{mod}\ \boldsymbol{n}$ hesaplanır. $\boldsymbol{s} = \boldsymbol{0}$ ise 1. adıma geri gidilir.
6. *A* kullanıcısı *m* mesajı için $(\boldsymbol{r}, \boldsymbol{s})$ çifti ile sayısal imzasını oluşturmuştur. Mesajla beraber alıcıya $(\boldsymbol{r}, \boldsymbol{s})$ de gönderilir.

Hash değerinin hesaplanmasında Secure Hash Algorithm (SHA) kullanılması önerilir. ANSI X9.30 standardında tanımlanan Secure Hash Algorithm SHA1 algoritması kullanılarak, 160 bit uzunluğundaki hash değerinin karşılığı olan tamsayı değeri kullanılır.

4. İmza Doğrulama

B kullanıcısının, *m* mesajı ile beraber gelen *A* 'nın sayısal imzası $(\boldsymbol{r}, \boldsymbol{s})$ 'i doğrulayabilmesi için; *A* 'nın kullandığı alan parametrelerini $\boldsymbol{D} = (\boldsymbol{q}, \boldsymbol{FR}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{G}, \boldsymbol{n}, \boldsymbol{h})$ ve *A* 'nın açık anahtar bilgisi olan *Q*'yu bilmesi gerekir. *B* 'kullanıcısının öncelikle *D* ve *Q* için doğrulama işlemlerini yapması önerilir. *B* sırasıyla aşağıdaki işlemleri yapar:

1. $\boldsymbol{1} \leq \boldsymbol{r} \leq \boldsymbol{n} - \boldsymbol{1}$ ve $\boldsymbol{1} \leq \boldsymbol{s} \leq \boldsymbol{n} - \boldsymbol{1}$ 'nin doğrulaması yapılır.
2. $\overline{\boldsymbol{m}} = \boldsymbol{SHA1}(\boldsymbol{m})$ hesaplanır.
3. $\boldsymbol{w} = \boldsymbol{s^{-1}} \boldsymbol{mod}\ \boldsymbol{n}$ hesaplanır
4. $\boldsymbol{u_1} = \overline{\boldsymbol{m}}.\boldsymbol{w}\ \boldsymbol{mod}\ \boldsymbol{n}$ ve $\boldsymbol{u_2} = \boldsymbol{r}.\boldsymbol{w}\ \boldsymbol{mod}\ \boldsymbol{n}$ hesaplanır
5. $(\boldsymbol{x_1}, \boldsymbol{y_1}) = \boldsymbol{u_1}\ \boldsymbol{G} + \boldsymbol{u_2}\ \boldsymbol{Q}$ hesaplanır
6. $\boldsymbol{x} = \boldsymbol{0}$ ise imza kabul edilmez , $\boldsymbol{x} \neq \boldsymbol{0}$ ise: $\overline{\boldsymbol{x_1}}$ tamsayı değerine çevrilerek $\boldsymbol{x_1}$ bulunur.
7. $\boldsymbol{v} = \overline{\boldsymbol{x_1}}\ \boldsymbol{mod}\ \boldsymbol{n}$ değeri bulunur
8. $\boldsymbol{v} = \boldsymbol{r}$ ise imza doğrulanmış olur.

İmzanın doğrulanmasına ilişkin yukarıdaki algoritmanın doğruluğu ispat edilebilir:

Eğer *m* mesajı için $(\boldsymbol{r}, \boldsymbol{s})$ imzası *A* kullanıcısı tarafından oluşturulduysa:

$\boldsymbol{s} = \boldsymbol{k^{-1}}(\overline{\boldsymbol{m}} + \boldsymbol{dr})\ \boldsymbol{mod}\ \boldsymbol{n}$ dir ve $\boldsymbol{k} = \boldsymbol{s^{-1}}\overline{\boldsymbol{m}} + \boldsymbol{s^{-1}}\boldsymbol{dr} = \boldsymbol{w}\overline{\boldsymbol{m}} + \boldsymbol{wdr}$
$= \boldsymbol{u_1} + \boldsymbol{u_2}\ \boldsymbol{d}\ \boldsymbol{mod}\ \boldsymbol{n}$ 'dir.

Böylelikle $\boldsymbol{u_1}\ \boldsymbol{G} + \boldsymbol{u_2}\ \boldsymbol{Q} = (\boldsymbol{u_1} + \boldsymbol{u_2}\ \boldsymbol{d})\ \boldsymbol{G} = \boldsymbol{kG}$, ve $\boldsymbol{v} = \boldsymbol{r}$ olmalıdır.

EDDSA

Edwards-eğrisi Dijital İmza Algoritması (EdDSA), Twisted Edwards eğrileri ile Schnorr imzasının bir geliştirmesini kullanarak dijital bir imza oluşturmak için kullanılır [30]. EDDSA, ECDSA'yı ve diğer imza şemalarını tehdit eden yaygın saldırıların çoğuna karşı bağışıklık kazanmak için inşa edilmiştir. Edwards eğrisi denklemi şu şekildedir;

$$\boldsymbol{ax^2 + y^2 = 1 + dx^2y^2}$$

EdDSA, mevcut imza şemalarına göre birçok avantaja sahip modern bir eliptik eğri imza şemasıdır. EdDSA'nın avantajları aşağıdaki gibidir:

- EdDSA, çeşitli platformlarda yüksek performans sağlar;
- Her imza için benzersiz bir rastgele numara kullanılması gereklidir;
- Yan kanal saldırılarına karşı daha dirençlidir [31].

EdDSA algoritması kullanılarak anahtar oluşturma, imzalama ve imza doğrulama aşamaları aşağıda yer verilmiştir.

1. Anahtar oluşturma

A kullanıcısı için anahtar çifti, ortam için tanımlanan eliptik eğri tabanlı alan parametreleri

$\boldsymbol{D = (q, Fq, A, B, c, l, k, h)}$ kullanılarak oluşturulur. *A* kullanıcısı anahtar çiftini oluşturmak için;

a. $\boldsymbol{A \in (Fq)\ ,\ B \in (Fq)}$
b. $\boldsymbol{E(Fq) = 2^c l}$ ve $\boldsymbol{2^{b-1} > q}$ olmalıdır [30].

2. İmza oluşturma

EdDSA imzalama algoritması M mesajın alınarak imzalayanın EdDSA özel anahtarı alınır ve çıktı olarak bir çift tamsayı $(\boldsymbol{R, s})$ üretilir. Açık anahtar *A* , $\boldsymbol{A \in (Fq)}$, $\boldsymbol{2b\ bit}$, $\boldsymbol{R \in (Fq)}$, ve $\boldsymbol{0 < S < l}$ dir.

1. $\boldsymbol{A = sB}$, $\boldsymbol{s = H_{0,\dots,b-1}(k)}$
2. $\boldsymbol{R = rB}$, $\boldsymbol{r = H\left(H_{b,\dots 2b-1}(k), M\right)}$ ve $\boldsymbol{S = R + H(R, A, M)s\ mod(l)}$

3. İmza Doğrulama

1. $\mathbf{2^C SB = 2^C(r + H(R, A, M)s)B}$

$\mathbf{= 2^C rB + 2^C H(R, A, M)sB}$

$\mathbf{= 2^C R + 2^C H(R, A, M)A}$

Ed25519 parametresi;

Ed25519 imzalar, güvenlikten ödün vermeden çok yüksek hızlara ulaşmak için çeşitli tasarım ve uygulama seviyelerinde özenle tasarlanmış Eliptik eğri imzalar olup en çok kullanılan bükülmüş Edwards eğrisidir [23]. Ed25519, 255 bitten oluşup, SHA-512 algoritmasını kullanan modern ve güvenli bir dijital imza algoritmasıdır. EdDSA algoritması Schnorr imza algoritmasına dayanır [31].

1. $\boldsymbol{q = 2^{255} - 19}$
2. $\boldsymbol{E/Fq}$, bükülmüş Edwars eğrisi,
3. $\boldsymbol{-x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2}$
4. $\boldsymbol{l =}$ $\mathbf{2\text{^}252 +}$ $\mathbf{27742317777372353535851937790883648493}$ **ve** $\boldsymbol{c = 3}$
5. $\boldsymbol{H(SHA - 512)}$, $\boldsymbol{b = 256}$
6. $\boldsymbol{x = \frac{u}{v}\sqrt{486664},\ y = \frac{u-1}{u+1}}$

[32].

ECDSA ve EDDSA'NIN KARŞILAŞTIRILMASI

Tablo 5- *ECDSA ve EDDSA' nın Karşılaştırılması*

İmzalama Algoritması	**Özet algoritması**	**Anahtar oluşturma**	**İmza oluşturma**	**İmza Doğrulama**
ECDSA	SHA-256	1 eliptik eğri çarpımından oluşmuştur.	3 eliptik eğri çarpımı, 1 toplama ve 1 modüler ters alma	2 eliptik eğri çarpımı ve 1 toplama ve 1 modüler ters alma, 2 modüler

				çarpma.
EdDSA	SHA-512	1 eliptik eğri çarpım	3 eliptik eğri çarpımı ve 1 toplama.	3 eliptik eğri çarpımı ve 1 toplama ve 3 tane modüler çarpma

Tablo 5'te görüldüğü üzere ECDSA ve EDDSA imzalama algoritmalarında kullanılan anahtar oluşturma, imza oluşturma ve imza doğrulamanı toplam kaç çarpma, toplama ve modüler ters alma işlemlerinden oluştuğu verilmiştir. EdDSA, diğer imza şemalarına kıyasla geliştirilmiş güvenliği ve performansı nedeniyle daha çok tercih edilmekle birlikte diğer birçok dijital imza yönteminden daha hızlı ve güvenlik açısından daha güçlüdür.

SONUÇ

Bilim ve teknolojinin paralel hızla ilerlemesi ve gelişmesi sonucunda, günümüzde bilgilerin istenmeyen kişi veya kişilerden korunması önemli bir konu halini almıştır. Bu durum bilgilerin korunması ve güvenli iletişim gibi kavramlar üzerinde yapılan çalışmaların daha da artmasına sebep olmuştur. Çalışmalar göstermiştir ki; güvenli bir iletişim ortamı oluşturmak için güçlü kriptosistemlere ihtiyaç vardır. Bu nedenle, simetrik ve asimetrik kriptosistemlerin önemi hızla artmaktadır.
Asimetrik kriptosistemler, simetrik kriptosistemlerden farklı olarak şifreleme ve deşifreleme işlemleri için iki ayrı anahtar kullanırlar. Asimetrik kriptosistemlerin, en güvenilir ve son zamanlardaki en popüler sistemi Eliptik Eğri Kriptosistemidir. Eliptik eğri kriptosistemi eliptik eğrileri temel alıp, bu eğriler üzerindeki noktalarla işlem yapar. Bu kriptosistem, diğer bir asimetrik kriptosistem olan RSA ile karşılaştırıldığında eşit güvenlik seviyesinde, daha küçük anahtar uzunluğu gerektirir. Daha küçük anahtar uzunluğu kullanımı, bilgisayar kaynaklarının sınırlı olduğu durumlarda üst düzey performans sağlar. Bu nedenle günümüzde önemi artmakta olan sayısal imza gibi akıllı kart kullanılan uygulamalarda eliptik eğri sistemi tercih edilmektedir. Temelde eliptik eğri kullanan birçok kripto sistem geliştirilmiş ve uygulamaya geçirilmiştir. Bu kripto sistemlerden uygulanabilirlik açısından uygun ve hızlı olan ECDSA ve EdDSA imzalama algoritmaları kullanılır. Blokzincirde yapılan işlemlerde bu imzalama algoritmaları kullanılır. EdDSA, ECDSA'yı ve diğer imza şemalarını tehdit eden yaygın

saldırıların çoğuna karşı bağışıklık kazanmak için inşa edilmiştir. EdDSA, mevcut imza şemalarına göre birçok avantaja sahip modern bir eliptik eğri imza şemasıdır. EdDSA, diğer imza şemalarına kıyasla geliştirilmiş güvenliği ve performansı nedeniyle daha çok tercih edilmekle birlikte diğer birçok dijital imza yönteminden daha hızlı ve güvenlik açısından daha güçlüdür. Bu çalışmada bu imzalama yöntemleri ele alınıp birbirlerine olan karşılaştırmaları verilmiştir.

KAYNAKLAR

[1]. Akben, S.B., Subaşı, A. (2005), RSA Ve Eliptik Eğri Algoritmasının Performans Karşılaştırması, KSÜ Fen Ve Mühendislik Dergisi , 35-40.

[2]. Atay, S. (2005), Eliptik Eğri Tabanlı Kriptografik Protokol ve Kart Üzerinde Bir Uygulama, İzmir İleri Teknoloji Enstitüsü, Bilgisayar Bölümü, İzmir.

[3]. Atay, S.(2006), Eliptik Eğri Kriptosistem Yazılım Uygulamalarında Hız Problemi, Doktora Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İzmir.

[4]. American Bankers Association, 1999, ANSI X9.62-1998: Public Key Cryptography for the Financial Services Industry: the Ellipti Cun/e Digital Signature Algorithm (ECDSA)

[5]. Draft NIST Special Publication 800-57, Recommendations for Key-Management, 2012.

[6]. Erözel durbilmez, S. (2018), Blockchaın Teknolojisinin Finans Sektöründeki Yeri ve Uygulamaları, Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü , İşletme Anabilim Dalı, İstanbul.

[7]. Houria, A., Abdelkader, B.M., Abderrezak, K. (2019), A Comparison Between The Secp256r and The Koblitz Secp256k1 Bitcoin Curves, Indonesian Journal Of Electrical Engineering And Computer Science, ISSN: 2502-4752, Mart 2019, 910-918

[8]. lnstitude of Electrical and Electronics Engineers, 2000, IEEE P363: Standard Specifications for Public-Key Cryptography

[9]. ISO, 2002, ISO/IEC 15946-222002, Information Technology – Security Techniques –

Cryptographic techniques based on elliptic cun/es – Part 2: Digital Signatures

[10]. Jansma N., Arrendondo B., 2004. Performance Comparison of Elliptic Curve and RSA Digital Signatures, *Technical Report from Sun Microsystems Laboratories*. http://research.sun.com/projects/crypto/ CHES_2004.pdf.

[11]. Johnson, D., Menezes, A., Vanstone, S. (2001), TheElliptic Curve Digital SignatureAlgorithm (ECDSA), july ,Springer-Verlag, 36-63, Canada.
[12]. Khalique, A., Singh, K., Sood, S. (2010), Implementation of Elliptic Curve Digital Signature Algorithm, *International Journal of Computer Applications*, 21-27. Hindistan.
[13]. Koblitz N. (1987), Elliptic Curve Cryptosystem. *Mathematics of Computation*, Vol. 48: 203-209.
[14]. Koblitz, N. "Algebraic Aspects of Cryptography", 1999, s.134 – 136.
[15]. Kurt, M. (2012), Eliptik Eğri Şifreleme Algoritmasının Uygulaması ve Analizi, Yüksek Lisans Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Edirne.
[16]. Menezes A. J., Oorschot P. C. V. ve Vanstone S. A. **(**1997), Handbook of Applied Cryptography. CRC Press, Boca Raton, Florida, USA.
[17]. Miller V. (1985), Uses of Elliptic Curves in Cryptography. *In H. C. Willams, Editor, Advances in Cryptology: CRYPTO'85, volume 218 of Lectures Notes in Computer Science, Springer-Verlag*. 417-426.
[18]. Murat, M. (2018), Blockchaın ile Güvenli Elektronik Sağlık Sistemi, Yüksek Lisans Tezi, İstanbul Üniversitesi Bilişim Enstitüsü, İstanbul.

[19]. NAKAMOTO, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[20]. NESSIE Consortium, (2003) NESSIE Security Report, *Technical report NESSIE.*
http://www.cosic.esat.kuleuven.ac.be/ nessie/ deliverables/ D20-v2.pdf
[21]. Rhee Man Y. (2003), Internet Security - Cryptographic principles, algorithms and protocols, Wiley
[22]. Rivest R. L., Shamir A. ve Adleman L. **(**1978), A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM,* **21(2)**:120-126, February 1978.
[23]. Romailler, Y., Pelissier, S. (2017), Practical Fault Attack Against The Ed25549 and Eddsa Signature Schemes, İsviçre.
[24]. Sarıkaya, K. (2005), Elektronik İmza Güvenliği ve Güvenlik Standartları Çerçevesinde
Düzenleyici Yaklaşımlar, Uzmanlık Tezi, Ankara.

[25]. SEC2"Standards for Efficient Cryptography Group": Recommended Elliptic Curve Domain Parameters. Version 1.0, 2000.
[26]. Yavuz, İ., (2008), Eliptik Eğri Kriptosisteminin FPGA Üzerinde Gerçeklenmesi, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, Elektronik Ve Haberleşme Mühendisliği Anabilim Dalı, İstanbul.
[27]. Yerlikaya, T., Aslan Yürek, C. (2019), RSA Algoritmasının Şifreleme Hızını Artıran Algoritmalar ve Performansları, Dümf Mühendislik Dergisi, 853-862.
[28]. Yerlikaya, T., Buluş, E., Arda, D.,(2005), Eliptik Eğri Şifreleme Algoritması Kullanan Dijital İmza Uygulaması, Trakya Üniversitesi, Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü, Edirne .
[29]. Yücelen, A.M., Baykal, A., Coşkun, D. (2017), Kriptolojide Eliptik Eğri Algoritmasının Uygulanması, Dicle Üniversitesi Mühendislik Fakültesi Dergisi, Temmuz, 503-514.
[30]. Josefsson, S., Liusvaara, I. (Ocak 2017). Edwards-Curve Dijital İmza Algoritması (EdDSA) . İnternet Mühendisliği Görev Gücü . doi : 10.17487 / RFC8032 . ISSN 2070-1721 . RFC 8032 . Erişim tarihi: 15.02.2020.
[31]. Bernstein, Daniel J.; Duif, Niels; Lange, Tanja; Schwabe, Peter; Bo-Yin Yang (2012). "Yüksek hızlı, yüksek güvenlikli imzalar" (PDF) . Kriptografik Mühendislik Dergisi . 2 (2): 77-89.
[32]. Bernstein, Daniel J.; Lange, Tanja (2007). Kurosawa, Kaoru (ed.). Eliptik eğrilerde daha hızlı ekleme ve iki katına çıkma .Kriptolojideki gelişmeler - ASIACRYPT. Bilgisayar Biliminde Ders Notları. 4833 . Berlin: Springer. s. 29–50.