MATEMATİKSEL MODELLEME, OPTİMİZASYON TEKNİKLERİ VE YAPAY ZEKA:

GÜNCEL ÇALIŞMALAR 1

$$f(x) = \sum_{i=1}^{n} w_i \phi_i(x) + \varepsilon$$

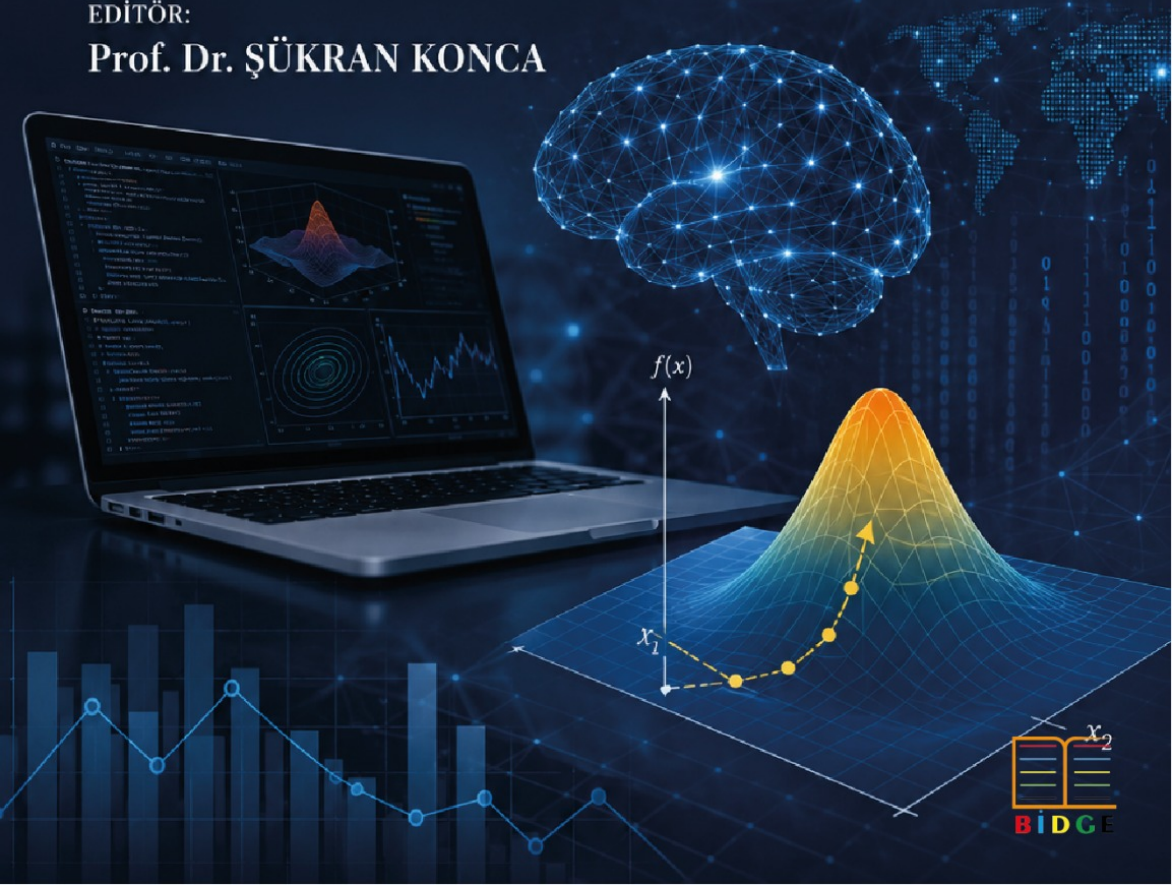
$$\frac{dx(t)}{dt} = Ax(t) + Bu(t)$$

$$\min_x f(x) \text{ s.t. } g(x) \le 0,, \; h(x) = 0$$

$$L(x, \lambda, \mu) = f(x) + \sum_{i=1}^{m} \lambda_i g_i(x) + \sum_{j=1}^{p} \mu_j h_j(x)$$

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

EDİTÖR:
Prof. Dr. ŞÜKRAN KONCA



BİDGE

BİDGE Yayınları

Matematiksel Modelleme, Optimizasyon Teknikleri ve Yapay Zeka: Güncel Çalışmalar 1

Editör: ŞÜKRAN KONCA

ISBN: 978-625-8821-39-0

1. Baskı
Sayfa Düzeni: Gözde YÜCEL
Yayınlama Tarihi: 2026-06-25
BİDGE Yayınları

Sertifika No: 71374
Yayın hakları © BİDGE Yayınları
www.bidgeyayinlari.com.tr - bidgeyayinlari@gmail.com
Krc Bilişim Ticaret ve Organizasyon Ltd. Şti.
Güzeltepe Mahallesi Abidin Daver Sokak Sefer Apartmanı No: 7/9 Çankaya / Ankara

ÖNSÖZ

Matematiksel modelleme, optimizasyon teknikleri ve yapay zekâ, günümüzün karmaşık problemlerine çözüm üretmede önemli araçlar hâline gelmiştir. Farklı disiplinlerde kullanılan bu yöntemler, bilimsel araştırmalara ve uygulamalara önemli katkılar sunmaktadır.

Matematiksel modelleme, gerçek dünyadaki sistemlerin anlaşılması ve analiz edilmesinde güçlü bir araç olarak öne çıkarken; optimizasyon teknikleri, sınırlı kaynakların en etkin şekilde kullanılmasına yönelik çözümler geliştirmektedir. Yapay zekâ ise veri odaklı öğrenme ve karar verme yetenekleriyle bu alanları tamamlayarak daha güçlü, esnek ve akıllı sistemlerin tasarlanmasına olanak sağlamaktadır. Günümüzde bu üç alan arasındaki etkileşimin giderek artması, bilimsel araştırmaların ve endüstriyel uygulamaların yönünü belirleyen temel unsurlardan biri hâline gelmiştir.

Matematiksel Modelleme, Optimizasyon Teknikleri ve Yapay Zekâ: Güncel Çalışmalar 1 adlı bu kitap; sinyal işleme, lojistik, finans ve siber güvenlik gibi farklı alanlarda gerçekleştirilen güncel çalışmaları bir araya getirmektedir. Kitapta, doğrusal cebir tabanlı mikrofon dizilerinde kaynak ayrıştırma ve gürültü bastırma, kan dağıtım ağlarında rota optimizasyonu, finansal modelleme ve yapay zekâ destekli siber tehdit istihbaratı konularında güncel çalışmalara yer verilmiştir.

Bu eser, matematiksel yöntemlerin ve yapay zekâ uygulamalarının farklı problem alanlarında nasıl etkin biçimde kullanılabileceğini göstermeyi amaçlamaktadır. Kitabın, araştırmacılar, lisansüstü öğrenciler ve ilgili alanlarda çalışan profesyoneller için faydalı bir kaynak olması en büyük temennimizdir.

Bu çalışmanın ortaya çıkmasına katkı sağlayan tüm bölüm yazarlarına ve yayın sürecinde emeği geçen herkese teşekkür ederiz.

Prof. Dr. Şükran KONCA

İÇİNDEKİLER

BÖLÜM 1

DOĞRUSAL CEBIR TABANLI MIKROFON DIZILERINDE KAYNAK AYRIŞTIRMA VE GÜRÜLTÜ BASTIRMA

MUSTAFA KEMAL AYDIN[1]
ŞÜKRAN KONCA[2]

1. Giriş

Bir akustik ortamda, K adet ses kaynağının karışımını kaydeden M elemanlı bir mikrofon dizisi düşünelim. Her mikrofon, istenen sinyal ile istenmeyen seslerin doğrusal bir karışımını kaydeder. Amacımız, doğrusal cebir tekniklerini kullanarak bu karışımdan istenen sinyali en iyi şekilde tahmin etmektir.

Bu problem, sinyal işleme literatüründe huzmeleme (beamforming) olarak bilinir ve günümüzde akıllı hoparlörler, işitme cihazları, video konferans sistemleri ve sesli asistanlar gibi birçok

[1]Yüksek Lisans Öğrencisi, İzmir Bakırçay Üniversitesi, Mühendislik Fakültesi, Akıllı Sistemler Mühendisliği Bölümü. E-posta: 6016095@bakircay.edu.tr Orcid:0009-0000-0306-9730

[2] Prof. Dr., Izmir Bakircay University, Faculty of Engineering and Architecture, Department of Fundamental Sciences, Izmir, Türkiye, sukran.konca@bakircay.edu.tr Orcid: 0000-0003-4019-958X

uygulamada kullanılmaktadır (Van Veen & Buckley, 1988; Benesty vd., 2008).

Günlük yaşamdan örnekler vermek gerekirse: akıllı hoparlörler (Alexa, Google Home) kullanıcıyı odanın neresinde olursa olsun duyabilir; video konferans sistemleri konuşan kişinin sesini odaklar ve arka plan gürültüsünü bastırır; işitme cihazları karşınızdaki kişinin sesini güçlendirirken arkadaki gürültüyü bastırır. Tüm bu uygulamaların temelinde, bu çalışmada incelenecek olan doğrusal cebir tabanlı sinyal ayrıştırma teknikleri yatar.

Tek bir mikrofonla farklı yönlerden gelen sesleri ayırmak mümkün değildir — mikrofon her yöne eşit duyarlıdır. Oysa birden fazla mikrofon, sesin yönünü ve konumunu belirlemeye olanak tanır. Mikrofon dizileri, her mikrofona ulaşan sesin zaman farklarını kullanarak uzaysal filtreleme yapar. Bu uzaysal filtreleme işlemine huzmeleme denir.

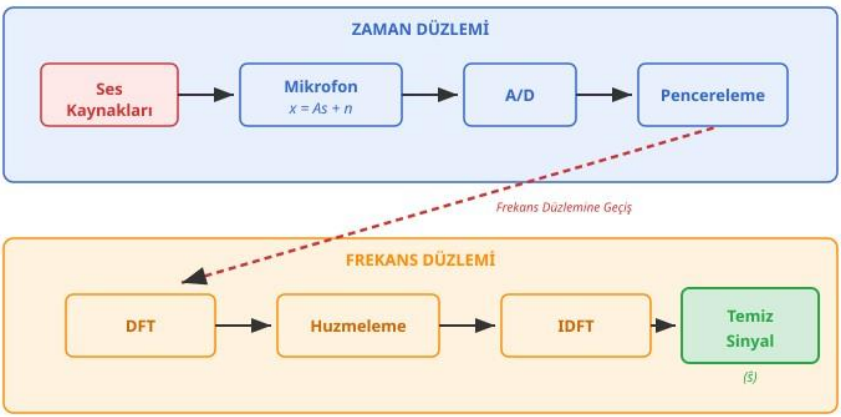
Bir odada konuşan bir insan düşünün. Odada aynı anda çalışan bir klima, dışarıdan gelen trafik sesi ve belki başka konuşan insanlar var. Siz sadece o tek kişinin sesini duymak istiyorsunuz. Mikrofon dizileri işte tam olarak bu sorunu çözer: birçok sesin karışımından sadece istediğiniz sesi ayıklar. Bu işlem, matematiksel olarak doğrusal cebir kullanılarak ifade edilir ve çözülür.

Matematiksel modeli kurarken şu varsayımlar yapılmıştır: (i) Kaynaklar uzak alandadır — dalga cephesi düzlemseldir. (ii) Ortam yayılımı doğrusal ve kayıpsızdır (sönümlenme ihmal edilir). (iii) Sinyaller durağandır; her frekans bini bağımsız olarak işlenebilir. (iv) Gürültü toplamsaldır ve sıfır ortalamalıdır. (v) Mikrofon sayısı kaynak sayısından büyük veya eşittir ($M \geq K$). Bu varsayımlar altında doğrusal cebir çerçevesiyle tam ve tutarlı bir çözüm elde edilebilir.

Bu çalışmada incelenecek ana yöntemler: Geciktir-ve-Topla (DAS), eşleşmiş filtre, en küçük kareler (LS), genelleştirilmiş en

küçük kareler (GLS), MVDR (Capon) huzmeleyici, MMSE tahmincisi ve ridge regresyonudur.

Çalışmanın ilerleyişi şu şekildedir: Önce zaman ve frekans düzlemlerinde sinyal modeli kurulacak, ardından mikrofon dizisi geometrisi ve yönlendirme vektörü tanımlanacaktır. Daha sonra huzmeleme kavramı ve DAS yöntemi açıklanacak, çok kaynaklı sistem için dizi manifold matrisi tanıtılacaktır. En küçük kareler çözümünün eksiksiz türetimi sunulacak ve dört mikrofonlu bir sistem üzerinde sayısal örnek verilecektir. Son olarak, gürültü kovaryans yapısının etkisi (GLS), MVDR huzmeleyici, regülarizasyon (ridge regresyonu) ve ileri konular incelenecektir.



Şekil 1: Sistemin genel iş akışı

2. Matematiksel Sistemin Kurulumu

2.1. Zaman Düzlemi Sinyal Modeli

M adet mikrofonlu bir dizide, m. mikrofonun n. örneğindeki sinyal x_m[n] ile gösterilsin. Her mikrofon sinyali, kaynakların gecikmeli bir toplamı artı gürültüdür:

$$x_m[n] = \Sigma_{k=1}^{K} h_{m,k}\, s_k[n - \tau_{m,k}] + n_m[n]$$

Burada $s_k[n]$, k. ses kaynağın sinyali; $h_{m,k}$ iletim katsayısı; $\tau_{m,k}$ yayılım gecikmesi; $n_m[n]$ gürültüdür. Uzak alan ve kayıpsız ortamda $h_{m,k} \approx 1$ alınır.

Zaman düzlemindeki gecikme, doğrusal olmayan bir kaydırma olduğu için analizi karmaşıklaştırır. Oysa frekans düzleminde basit bir karmaşık çarpıma dönüşür. Bu nedenle sinyaller DFT ile frekans düzlemine taşınır (Cooley & Tukey, 1965). N noktalı Ayrık Fourier Dönüşümü (DFT), ayrık zamanlı bir sinyali frekans düzlemine dönüştürmek için kullanılır. N noktalı DFT şu şekilde tanımlanır:

$$X_m[k] = \sum_{n=0}^{N-1} x_m[n] e^{-j\frac{2\pi}{N}kn}.$$

Burada:

- $x_m[n]$: m'inci mikrofonun zaman düzlemindeki sinyali,
- $X_m[k]$: aynı sinyalin k'ncı frekans bileşeni,
- N: DFT uzunluğu (örnek sayısı),
- n: zaman örnek indeksi,
- k: frekans bin indeksi,
- $j = \sqrt{-1}$: sanal birimdir.

Bu dönüşüm, ayrık zamanlı sinyali frekans bileşenlerine ayırır.

2.2. Frekans Düzlemine Geçiş

DFT'nin gecikme özelliği sayesinde zaman düzlemindeki τ gecikmesi, frekans düzleminde bir faz kaymasına dönüşür:

$$\{s[\mathrm{n} - \tau]\} \rightarrow S[k] \cdot e^{-\mathrm{j}\omega\tau}$$

Her frekans bini bağımsız işlenebildiği için, tek bir ω frekansına odaklanılır. Tüm nicelikler bu frekansta karmaşık değerli sabitler

(fazörler) olur. Karmaşık sayı (fazör) $Ae^{j\phi}$ formundadır; A genlik, φ faz açısıdır. $e^{j\omega\tau}$ çarpanı sinyale faz kayması uygular, genliğini değiştirmez.

Frekans düzleminde ölçüm modeli şu olur:

$$X_m(\omega) = \sum_{k\prime=1}^{K} S_{k\prime}(\omega)\, e^{-j\omega\tau(m,k\prime)} + N_m(\omega).$$

Burada $S_{k'}(\omega)k'$kaynağının frekans bileşeni, $\tau(m,k')$ yayılım gecikmesi ve $N_m(\omega)$gürültüdür.

Tüm nicelikler karmaşık sayılardır. Faz bilgisi sesin yönünü belirlemede kritik önem taşır: farklı yönlerden gelen sinyaller farklı faz kaymaları üretir ve bu kaymalar yönlendirme vektörü tarafından kodlanır.

Süperpozisyon prensibi sayesinde, frekans düzleminde her bin bağımsız olarak işlenebilir. Bu, karmaşık çok kaynaklı problemleri tek frekans için çözülebilir alt problemlere böler. Tüm türetimler tek bir ω frekansı için yapıldıktan sonra, sonuçlar tüm frekans binleri için genelleştirilir. Bu yaklaşım, geniş bant sinyal işlemenin temelidir.

Fourier dönüşümünün bu güçlü özelliği, doğrusal olmayan zaman düzlemi işlemlerini (gecikme, kaydırma) doğrusal frekans düzlemi işlemlerine (karmaşık çarpma) dönüştürür. Bu sayede tüm sistem doğrusal bir matris denklemi olarak ifade edilebilir ve doğrusal cebirin tüm araçları (matris tersi, sözde ters, özdeğer ayrışımı vb.) kullanılarak çözülebilir.

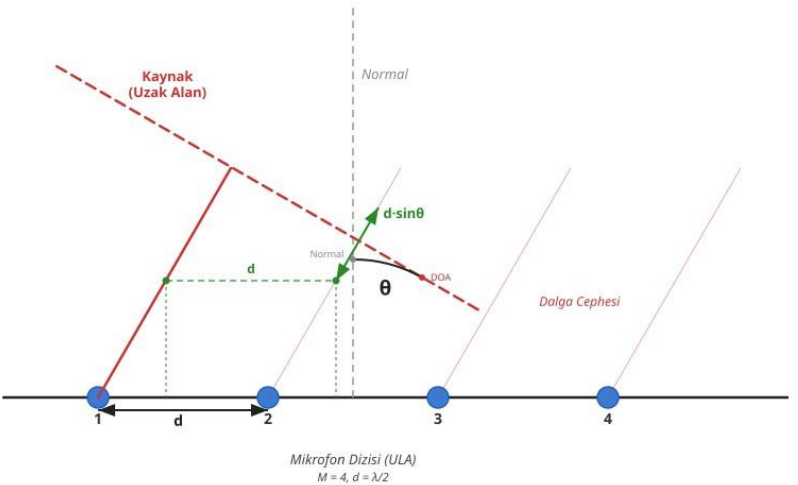
3. Mikrofon Dizisi Geometrisi ve Yönlendirme Vektörü

3.1. Dalga Yayılımı ve Zaman Gecikmesi

Uzak alandaki kaynaktan yayılan ses, diziye düzlemsel dalga cephesi olarak ulaşır. θ açısından gelen dalga için m. mikrofondaki zaman gecikmesi:

$$\tau_m(\theta) = d_m \sin\theta / c$$

Burada c ≈ 340 m/s ses hızıdır. θ = 0° (broadside) durumunda gecikme sıfırdır; θ = ±90° (endfire) durumunda maksimumdur.



Şekil 2: ULA geometrisi ve dalga cephesi

3.2. Yönlendirme Vektörü

M elemanlı dizi için θ yönündeki kaynağın yönlendirme vektörü (Van Trees, 2002):

$$a(\theta) = [1,\ e^{-j\omega\tau_2(\theta)},\ e^{-j\omega\tau_3(\theta)},\ \ldots,\ e^{-j\omega\tau_m(\theta)}]^T$$

Her bileşenin büyüklüğü 1'dir. Bu vektör kaynağın uzaysal imzasıdır (spatial signature). Yönlendirme vektörü, belirli bir θ yönünden gelen kaynağın tüm mikrofonlarda yarattığı faz kaymalarını tek bir vektörde toplar. Hangi açıdan ses geliyorsa,

yönlendirme vektörü farklı olur. Bu vektör, huzmeleme ve kaynak ayrıştırma işlemlerinin temel yapı taşıdır.

3.3. Tekdüze Doğrusal Dizi (ULA)

Mikrofonların eşit d aralığıyla dizildiği ULA için d_m = (m−1)d (Balanis, 2016). d = λ/2 seçimi uzaysal örtüşmeyi önler. Bu seçimle yönlendirme vektörü sadeleşir:

$$a_m(\theta) = e^{-j(m-1)\pi \sin\theta}$$

Bu çalışmadaki değerler: f = 500 Hz, c = 340 m/s, λ = 0.68 m, d = 0.34 m = λ/2. Bu seçim yarım dalga boyu aralığı sayesinde uzaysal örtüşmeyi (spatial aliasing) önler. Uzaysal örtüşme, farklı yönlerden gelen sinyallerin aynı faz farkını üretmesi durumudur — tıpkı bir filmde tekerleklerin ters yönde dönüyormuş gibi görünmesine benzer. d = λ/2 seçimi bu belirsizliği ortadan kaldırır.

3.4. Sayısal Örnek

M = 4 mikrofonlu ULA için iki kaynak:

$a(0°) = [1, 1, 1, 1]$ $a(90°) = [1, -1, 1, -1]$

Bu iki vektör ortogonaldir: iç çarpımları 1−1+1−1 = 0. Bu özel durum çözümü büyük ölçüde kolaylaştırır. Pratikte kaynak açıları genellikle ortogonal değildir; bu durumda A*A matrisi köşegen olmaz ve çözüm daha karmaşık hale gelir.

4. Huzmeleme (Beamforming)

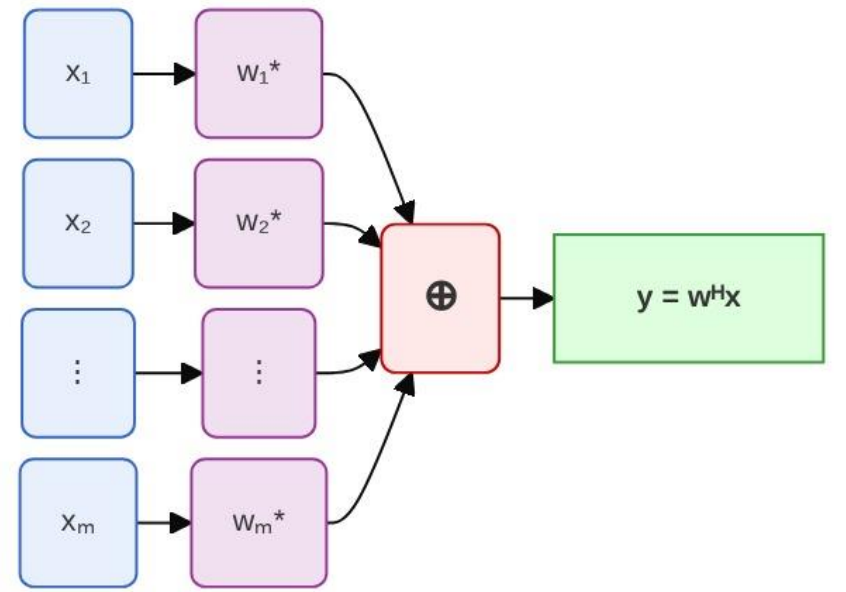
4.1. Tanım

Huzmeleme, mikrofon sinyallerinin doğrusal bir kombinasyonudur (Van Veen & Buckley, 1988). Huzmeleme işleminde her mikrofon sinyali bir ağırlık katsayısı ile çarpılır ve tüm

çarpımlar toplanır. Ağırlıklar, odaklanmak istenen yöne göre belirlenir. Çıkış:

Ağırlık vektörü w'yi akıllıca seçerek istediğimiz yöndeki sinyali güçlendirebilir, istenmeyen yönleri ise zayıflatabiliriz. Bu, bir kameranın lensini bir yöne odaklamasına benzer — sadece belirli bir yönden gelen sesi netleştirip diğer yönleri bulanıklaştırır. Huzmeleyicinin kalitesi, ağırlık vektörünün ne kadar iyi seçildiğine bağlıdır.

$$y = \Sigma_{m=1}^{M} w_m^* x_m = w^H x$$



Şekil 3: Huzmeleyici blok diyagramı

4.2. Geciktir-ve-Topla (DAS)

DAS, yönlendirme vektörünü ağırlık olarak kullanır:

$$w_{DAS}(\theta) = (1/M)\, a(\theta)$$

İstenen yönden gelen sinyal yapıcı girişim yapar; diğer yönler yıkıcı girişimle bastırılır. DAS'in iki adımı vardır: (1) Geciktir — her mikrofon sinyalini karşılık gelen faz kaymasıyla düzelt. (2) Topla — tüm düzeltilmiş sinyalleri topla. İstenen yönden gelen sinyal tüm kanallarda aynı fazda olduğu için üst üste binerek güçlenir; diğer yönlerden gelen sinyaller farklı fazlarda olduğu için birbirini söndürür.

DAS, en eski ve en basit huzmeleme yöntemi olmasına rağmen, günümüzde hala birçok uygulamada kullanılmaktadır. Basitliği ve hesaplama verimliliği onu özellikle gerçek zamanlı sistemler için cazip kılar. Ancak DAS'in bir dezavantajı vardır: yan huzmeleri (side lobes) yüksektir, yani istenen yön dışındaki yönlerden gelen sinyalleri tam olarak bastıramaz. Bu sorunu çözmek için daha gelişmiş yöntemler (MVDR, MMSE) geliştirilmiştir.

4.3. Eşleşmiş Filtre ve SNR Maksimizasyonu

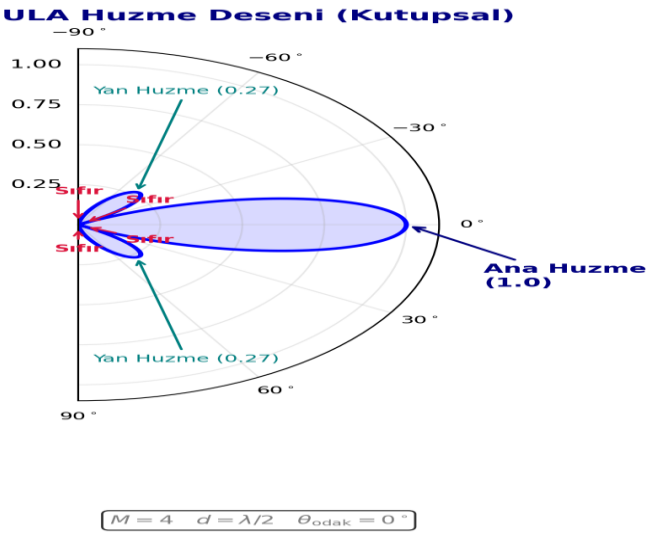
Tek kaynak ve gürültülü durumda çıkış SNR'ı:

$$SNR_{out} = |w^H a(\theta)|^2 \sigma_s^2 / (w^H R_n w)$$

Beyaz gürültüde ($R_n = \sigma_n^2 I$), Cauchy–Schwarz eşitsizliğinden $\mathrm{SNR} \leq M \cdot \mathrm{SNR_{in}}$ bulunur. Cauchy–Schwarz eşitsizliği $|w^* a|^2 \leq (w^* w)(a^* a)$ ilişkisidir. Eşitlik ancak $w \propto a(\theta)$ için sağlanır. Bu, eşleşmiş filtredir (North, 1943; Turin, 1960): $w_{\mathrm{opt}} = a(\theta)$. Bu ağırlıkla çıkış sinyal gücü M²σ²_s, çıkış gürültü gücü Mσ²_n olur. Dolayısıyla

$$\mathrm{SNR} = \frac{M^2 \sigma_s^2}{M \sigma_n^2} = M \cdot \mathrm{SNR_{in.}}$$

M = 4 mikrofonla kazanç ~6 dB'dir. Bu sonuç, daha fazla mikrofonun daha iyi gürültü bastırma sağladığını gösterir; ancak maliyet ve karmaşıklık da artar.



Şekil 4: M = 4 ULA için kutupsal huzme deseni

5. Çoklu Kaynak Modeli ve Dizi Manifold Matrisi

K kaynak için frekans düzlemindeki doğrusal model (Schmidt, 1986):

$$x = As + n$$

Burada *x* (M×1) ölçüm, *A* (*M*×*K*) dizi manifold matrisi, s (*K*×1) kaynak, *n* (M×1) gürültü vektörüdür. A'nın sütunları yönlendirme vektörleridir.

A'nın sütunları yönlendirme vektörleridir: A = [a(θ₁) | a(θ₂) | ... | a(θ_K)]. Her sütun ilgili kaynağın uzaysal imzasını temsil eder ve tüm sistem, mikrofon dizisinin uzaysal örnekleme yapısını doğrusal cebir çerçevesinde ifade eder.

Örnek (*M* = 4, *K* = 2):

$$A = [1\ 1;\ 1\ -1;\ 1\ 1;\ 1\ -1], \quad A^H A = 4\mathrm{I}$$

A^*A'nın köşegen olması, yönlendirme vektörlerinin ortagonal olmasından kaynaklanır. H, Hermityen transpozu (karmaşık eşlenik transpoz) ifade eder. $M \geq K$ koşulu sağlandığında sistem aşırı belirlenmiştir — yani denklemden fazla bilinmeyen vardır ve tam çözüm yerine en iyi tahmini bulmamız gerekir. Bu, en küçük kareler yönteminin uygulama alanıdır.

Dizi manifold matrisinin rankı, kaynakların ayrıştırılabilirliğini belirler. Eğer iki kaynak aynı yönden geliyorsa ($\theta_1 = \theta_2$), yönlendirme vektörleri aynı olur ve A matrisinin rankı düşer. Bu durumda kaynaklar birbirinden ayrılamaz. Kaynakların ayrıştırılabilmesi için yönlendirme vektörlerinin doğrusal bağımsız olması (A'nın tam sütun ranklı olması) gerekir.

6. En Küçük Kareler Çözümü

6.1. Problem

$M \geq K$ durumunda x'ten s'yi tahmin için LS kullanılır (Gauss, 1809; Björck, 1996). LS, ölçümler ile model arasındaki karesel hatayı minimize eder:

$$J(s) = ||x - As||^2$$

Burada ||.|| Öklid normudur (vektör bileşenlerinin kareleri toplamı). $J(s)$'i açalım: $J(s) = (x - As)^*(x - As) = x^*x - x^*As - s^*A^*x + s^*A^*As$.

6.2. Normal Denklemler

Karmaşık değişkenler için Wirtinger kalkülüsü kullanılarak s* göre gradyan hesaplanır. Gradyan kuralları: sabit terimin gradyanı sıfır; s^*A^*x'nin gradyanı A^*x; s^*A^*As'nin gradyanı A^*As. Dolayısıyla:

$$\partial J/\partial s^* = -A^H x + A^H As = 0$$

Bu, normal denklemleri verir:

$$A^H A\, \hat{s} = A^H x$$

Geometrik anlamı: artık vektörü e = x − Aŝ, A'nın sütun uzayına dik olmalıdır (ortogonallik prensibi).

6.3. Çözüm ve Sözde Ters

A tam sütun ranklıysa çözüm:

$$\hat{s} = (A^H A)^{-1} A^H x = A^+ x$$

$A^+ = (A^*A)^{-1}A^*$ Moore–Penrose sözde tersidir (Moore, 1920; Penrose, 1955). Dört Penrose koşulunu sağlar: $AA^+A = A$, $A^+AA^+ = A^+$, $(AA^+)^* = AA^+$, $(A^+A)^* = A^+A$. Geometrik olarak, ŝ x'in A'nın sütun uzayına dik izdüşümüdür. Artık vektörü e = x − Aŝ, A'nın sütun uzayına diktir: $A^*e = A^*(x - A\hat{s}) = A^*x - A^*A(A^*A)^{-1}A^*x = 0$.

7. Sayısal Örnek: 4 Mikrofon, 2 Kaynak

7.1. Parametreler

M = 4, K = 2, d = λ/2. $\theta_1 = 0°$ ($s_1 = 1.0$ V), $\theta_2 = 90°$ ($s_2 = 0.5$ V). Gürültü: $\sigma^2\_n = 0.01$.

7.2. Ölçüm Vektörü

Gürültüsüz ölçüm: $x_0 = As = s_1 a(\theta_1) + s_2 a(\theta_2) = 1.0 \cdot [1, 1, 1, 1] + 0.5 \cdot [1, -1, 1, -1] = [1.5, 0.5, 1.5, 0.5]$. Bileşen bazında: $x_{01} = 1+0.5 = 1.5$; $x_{02} = 1-0.5 = 0.5$; $x_{03} = 1.5$; $x_{04} = 0.5$.

Şimdi $\sigma^2\_n = 0.01$ varyanslı karmaşık beyaz Gauss gürültüsü eklenir. Örnek gerçekleme: n = [0.010+0.011j, −0.020−0.029j, 0.015+0.009j, 0.018−0.033j]. Her bileşen için gerçek ve sanal kısımlar N(0, 0.005) dağılımına sahiptir. Gürültülü ölçüm:

$$x = [1.510+0.011j,\ 0.480-0.029j,\ 1.515+0.009j,\ 0.518-0.033j]^T$$

7.3. LS Çözümü

Adım 1 — $A^*A = \text{diag}(4, 4) = 4I_2$. (1,1) elemanı: 1+1+1+1 = 4. (1,2) elemanı: 1−1+1−1 = 0.

Adım 2 — A^*x hesapla. Birinci bileşen [1,1,1,1]x: gerçek 4.023, sanal −0.042; sonuç 4.023 − 0.042j. İkinci bileşen [1,−1,1,−1]x: gerçek 2.027, sanal 0.082; sonuç 2.027 + 0.082j.

Adım 3 — $(A^*A)^{-1} = (1/4)I$ olduğundan her bileşeni 4'e böl:

$$\hat{\mathbf{s}} = [1.006 - 0.011j,\ 0.507 + 0.021j]^T$$

İstenen kaynak tahmini 1.006 − 0.011j ≈ 1.01 V (gerçek 1.0 V). Parazit tahmini 0.507 + 0.021j ≈ 0.51 V (gerçek 0.5 V). Mutlak hatalar sırasıyla ~0.013 ve ~0.022'dir.

Bu tahminlerin başarısının üç temel nedeni vardır. Birincisi, A matrisi tam sütun ranklıdır (rank = 2 = K) ve iyi koşulludur (koşul sayısı $\kappa = 1$). İkincisi, iki yönlendirme vektörü ortogonal olduğu için kaynaklar arası girişim (cross-talk) yoktur. Üçüncüsü, gürültü varyansı ($\sigma^2\_n = 0.01$) sinyal genliklerine (1.0 ve 0.5 V) göre küçüktür — giriş SNR'ı yüksektir.

Tablo 1: LS tahmin sonuçları

Kaynak	Gerçek	Tahmin	Hata
s_1	1.000	1.006−0.011j	≈0.013
s_2	0.500	0.507+0.021j	≈0.022

Hatalar gürültü seviyesiyle uyumludur. Eğer mikrofon sayısı 2'ye düşürülseydi SNR kazancı 3 dB olurdu. Altı mikrofonla ~7.8 dB. Kaynak yönleri yakın olsaydı (örneğin 0° ve 10°), yönlendirme vektörleri ortogonal olmazdı ve ridge regresyonu gerekli olabilirdi.

8. Gürültü Kovaryans Yapısının Etkisi

Pratikte gürültü genellikle beyaz değildir. Yakın mikrofonlarda benzer çevresel gürültü, elektromanyetik girişim veya yankılanma, mikrofonlar arası korelasyona yol açar. Bu durumda R_n genel bir pozitif tanımlı matristir ve köşegen dışı elemanları sıfırdan farklıdır. Klasik LS bu durumda optimal değildir.

Genelleştirilmiş En Küçük Kareler (GLS), gürültü kovaryansını kullanan ağırlıklı LS'dir ve en iyi doğrusal yansız tahminciyi (BLUE) verir (Aitken, 1935):

$$\hat{\mathbf{s}}_{GLS} = (A^H R_n^{-1} A)^{-1} A^H R_n^{-1} x$$

Beyazlatma dönüşümü: $R_n^{-1} = L^*L$ (Cholesky ayrışımı). Dönüştürülmüş değişkenler $\tilde{x} = Lx$, $\tilde{A} = LA$ tanımlanırsa, dönüştürülmüş gürültünün kovaryansı $E[Ln(Ln)^*] = LR_nL^* = I$ olur — yani gürültü beyazlaşır. Artık klasik LS uygulanabilir. L matrisi gürültüyü düzleştirir: farklı yönlerde farklı varyanslara sahip dağılımı, tüm yönlerde eşit varyanslı hale getirir.

Özel durum: Beyaz gürültüde ($R_n = \sigma^2_n I$), GLS çözümü LS'ye indirgenir. GLS, LS'nin doğal bir genellemesidir.

Gürültü kovaryans matrisi $R_n = E[nn^*]$, gürültü vektörünün bileşenleri arasındaki ilişkiyi ölçer. Köşegen elemanları her mikrofondaki gürültü varyansını, köşegen dışı elemanları ise mikrofonlar arası kovaryansı temsil eder. Beyaz gürültüde köşegen dışı elemanlar sıfırdır — mikrofonlar birbirinden bağımsızdır. İlişkili gürültüde ise köşegen dışı elemanlar sıfırdan farklıdır ve bu bilgi GLS tarafından optimum şekilde kullanılır.

9. MVDR Huzmeleyici

MVDR çıkış varyansını minimize edip istenen yönde birim kazanç ($w^*a = 1$) korur (Capon, 1969). Optimizasyon problemi: min $w^*R_n w$ öyle ki $w^*a(\theta) = 1$.

Lagrange çarpanı yöntemiyle dört adımda çözülür: (1) Lagrange fonksiyonu tanımla. (2) w*'ya göre gradyanı sıfırla: R_n w = λ a(θ). (3) w = λ R_n^{-1} a(θ) bulun. (4) Kısıttan λ = 1/(a*R_n^{-1}a) hesapla. Sonuç:

$$w_{MVDR} = R_n^{-1}a / (a^H R_n^{-1}a)$$

LS kaynak ayrıştırma yöntemidir; MVDR uzaysal filtre tasarımıdır. LS x ölçümlerini kullanarak s kaynak sinyallerini birebir tahmin eder. MVDR ise gürültü istatistiklerini (R_n) kullanır ve çıkışı bir bütün olarak optimize eder.

Beyaz gürültüde MVDR, normalize eşleşmiş filtreye (w = a/M) indirgenir. MVDR, eşleşmiş filtrenin korelasyonlu gürültü için genelleştirilmiş halidir.

MVDR'nin en büyük avantajı, gürültü+parazit kovaryans matrisini kullanarak sadece beyaz gürültüyü değil, yönlü parazit kaynaklarını da otomatik olarak bastırabilmesidir. Eğer bir parazit kaynağı θ_p yönünden geliyorsa, MVDR o yönde düşük kazanç (null) oluşturur. Bu özellik, MVDR'yi DAS'a göre üstün kılar: DAS yan huzmelerde yüksek kazanç sağlarken, MVDR parazit yönlerinde kazancı sıfıra yakın tutar.

MVDR'nin pratikteki zorluğu, R_n matrisinin bilinmemesidir. R_n genellikle sinyalin bulunmadığı durumlarda (örneğin sessizlik dönemlerinde) ölçümden tahmin edilir. Bu tahminin doğruluğu, MVDR'nin performansını doğrudan etkiler. Yetersiz tahmin, sinyalin kendi yönünde de bastırılmasına (signal cancellation) yol açabilir.

MMSE tahmincisi E[||ŝ − s||²]'yi minimize eder (Wiener, 1949; Kailath vd., 2000): ŝ = R_sx R_xx^{-1} x. Burada R_sx sinyal-ölçüm çapraz kovaryansı, R_xx ölçüm kovaryans matrisidir. LS yalnızca ölçüm modelini kullanırken, MMSE hem sinyal hem gürültü istatistiklerini birlikte kullanır.

10. Regülarizasyon: Ridge Regresyonu

A*A kötü koşullu ise ridge regresyonu kullanılır (Tikhonov, 1963; Hoerl & Kennard, 1970). Kötü koşulluluk, kaynak yönleri birbirine yakınsa veya mikrofon geometrisi zayıfsa ortaya çıkar. Düzenlenmiş hata fonksiyonu: J_λ(s) = ||x − As||² + λ||s||². Gradyanı sıfıra eşitlenince:

$$\hat{s}_\lambda = (A^H A + \lambda I)^{-1} A^H x$$

λ > 0 matrisi her zaman pozitif tanımlı ve iyi koşullu yapar. Koşul sayısı κ(A*A + λI) ≤ (λ_max + λ)/λ ile sınırlıdır. λ → 0'da LS'ye yaklaşırlır; λ → ∞'da çözüm sıfıra yaklaşırlar.

Ridge regresyonu yanlı ama varyansı düşük bir tahmincidir. L-eğrisi, Genelleştirilmiş Çapraz Doğrulama (GCV) veya Morozov'un sapma ilkesi ile λ seçilir (Hastie vd., 2009). Ridge, özellikle az sayıda mikrofon veya yüksek gürültü seviyesi durumunda LS'den daha güvenilir sonuçlar üretir.

Ridge regresyonu ile LS arasındaki fark şöyle özetlenebilir: LS, çözümün yanlılığının (bias) sıfır olmasını amaçlar — yani çok sayıda gerçekleme yapıldığında tahminlerin ortalaması gerçek değere yakınsar. Ancak tek bir gerçeklemede varyans yüksek olabilir. Ridge ise küçük bir yanlılık kabul eder, bunun karşılığında varyansı önemli ölçüde azaltır. Toplam ortalama kare hata (MSE = yanlılık² + varyans), Ridge için daha düşük olabilir. Bu denge, istatistiksel öğrenmenin temel prensibi olan yanlılık-varyans dengesidir (bias-variance tradeoff).

11. İleri Konular

11.1. Uyarlamalı Huzmeleme

Bu çalışmadaki yöntemler gürültü istatistiklerinin (R_n) bilindiğini varsayar. Pratikte R_n ölçümlerden tahmin edilir.

Uyarlamalı algoritmalar (LMS, RLS, APA) bu tahmini çevrimiçi günceller (Haykin, 2014). Her örnekte ağırlıkları adım adım güncelleyerek değişen ortam koşullarına uyum sağlarlar.

11.2. Geniş Bant Sinyaller

Bu çalışma tek frekans içindir. Konuşma gibi geniş bant sinyaller için her frekans bininde bağımsız dar bant huzmeleyiciler kullanılır, çıkışlar ters DFT ile birleştirilir (overlap-add yöntemi).

11.3. Doğrusal Öngörü ile Fark

Doğrusal öngörü (LP), bir zaman serisinin gelecek değerini geçmiş değerlerinin doğrusal kombinasyonu ile tahmin eder (Makhoul, 1975). LP zamansal korelasyona dayanır; bu çalışmadaki LS ise uzaysal karışımı çözer. Her iki yöntem matematiksel olarak benzer formda olsa da, değişkenlerin fiziksel anlamı tamamen farklıdır. LP'nin A matrisi zaman gecikmeli sinyal değerlerinden oluşurken, kaynak ayrıştırmada A matrisi uzaysal yönlendirme vektörlerinden oluşur.

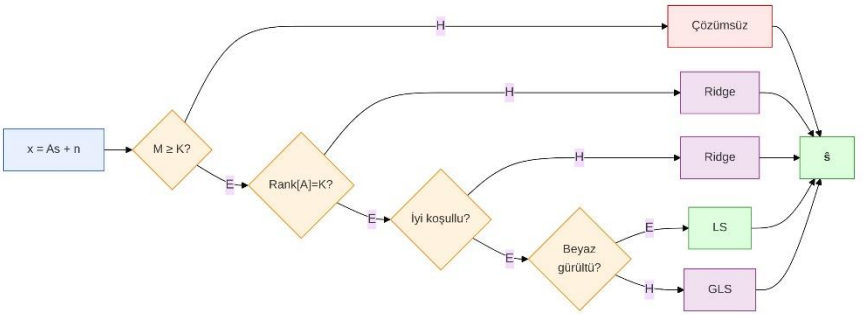
11.4. Genel Dizi Geometrileri

ULA en basit geometridir. Pratikte dairesel, dikdörtgensel veya rastgele diziler de kullanılır. Genel bir dizi için $\tau_m(\theta,\varphi)$, mikrofonun 3B konum vektörü p_m ve dalga yayılım yönü $k(\theta,\varphi)$ cinsinden ifade edilir: $\tau_m = -p_m k / c$. Dairesel diziler 360° arama kabiliyeti sağlarken, düzlemsel diziler 3B yön bulma imkanı sunar.

11.5. Uygulama Alanları

Mikrofon dizisi huzmeleme teknolojisi günümüzde geniş bir uygulama yelpazesine sahiptir. Akıllı hoparlörlerde (Amazon Echo, Google Home) sesli asistanları çevre gürültüsünden korur. Video konferans sistemlerinde (Zoom, Teams) uzaktaki konuşmacının sesini netleştirir. İşitme cihazlarında kullanıcıya yönelik sesi

güçlendirirken arka plan gürültüsünü bastırır. Otomotiv uygulamalarda sürücü sesini motor gürültüsünden ayırır. Tıbbi ultrason ve radar sistemlerinde benzer prensipler kullanılır.



Şekil 5: Çözüm yöntemi seçim akış diyagramı

Tablo 2: Çözüm yöntemleri özeti

Yöntem	Amaç	Çözüm
LS	min $\|\|x-As\|\|^2$	$(A^*A)^{-1}A^*x$
GLS	ağırlıklı LS	$(A^*R_n^{-1}A)^{-1}A^*R_n^{-1}x$
Ridge	regularized LS	$(A^*A+\lambda I)^{-1}A^*x$
MVDR	min w^*R_nw	$R_n^{-1}a/(a^*R_n^{-1}a)$
Eş.Filtre	max SNR	$w = a$

12. Sonuç

Bu çalışmada, mikrofon dizilerinde kaynak ayrıştırma ve gürültü bastırma probleminin doğrusal cebir çerçevesi eksiksiz türetilmiştir. Yönlendirme vektörü, dizi manifold matrisi, LS, GLS, MVDR ve ridge regresyonu yöntemlerinin matematiksel türetimleri sunulmuştur.

Sayısal örnek, iyi koşullu bir sistemde LS'nin başarılı tahminler ürettiğini göstermiştir. Gürültünün korelasyonlu olduğu

durumlarda GLS, matrisin kötü koşullu olduğu durumlarda ridge regresyonu gerekmiştir.

Bu çalışma, doğrusal cebirin sinyal işleme alanındaki güçlü uygulamasını göstermektedir. Matris işlemleri, sözde ters ve optimizasyon gibi temel kavramların pratik mühendislik problemlerine nasıl uygulanacağını ortaya koymaktadır.

Gelecek çalışmalarda uyarlamalı huzmeleme algoritmalarının gerçek zamanlı performans analizi, geniş bant sinyaller için çok kanallı yöntemlerin incelenmesi, derin öğrenme tabanlı sistemlerin doğrusal cebir yaklaşımlarıyla karşılaştırılması ve reverberant (yankılı) ortamlarda yankı giderme ile huzmelemenin birleştirilmesi planlanmaktadır.

13. Terimler Sözlüğü

Ağırlık vektörü (w): Mikrofon sinyallerini ağırlıklandıran karmaşık vektör.

Beyaz gürültü: Tüm frekanslarda eşit güç, bağımsız süreç. $R_n = \sigma^2_n I$.

Broadside: Dizi eksenine dik yön ($\theta = 0°$).

DAS: Delay-and-Sum: en basit huzmeleme. $w = (1/M)a(\theta)$.

DFT: Ayrık Fourier Dönüşümü: zamanı frekansa çevirir.

Dizi manifold (A): Yönlendirme vektörlerini sütun olarak içeren matris.

Endfire: Dizi eksenine paralel yön ($\theta = 90°$).

Eşleşmiş filtre: Beyaz gürültüde optimum: $w = a(\theta)$.

GLS: Genelleştirilmiş LS: korelasyonlu gürültü için.

Hermityen transpoz (H): Karmaşık eşlenik + transpoz.

Huzmeleme: Diziyi bir yöne odaklama.

Karmaşık sayı (fazör): a + jb, genlik ve faz taşır.

Koşul sayısı (κ): Matris kararlılık ölçüsü.

Kovaryans (R_n): Gürültü ikinci momenti: E[nn*].

LS: En küçük kareler: min $||x-As||^2$.

MMSE: Min. ort. kare hata tahmincisi.

Moore–Penrose ters (A^+): Genelleştirilmiş matris tersi.

MVDR (Capon): Min. varyans, bozulmasız huzmeleyici.

Normal denklemler: A*Aŝ = A*x.

Ortogonallik: İç çarpımın sıfır olması.

Parazit: İstenmeyen ses kaynağı.

Rank: Bağımsız satır/sütun sayısı.

Ridge regresyonu: λI ekleyerek düzenleme.

SNR: Sinyal/gürültü oranı. M mikrofonla M kat.

Süperpozisyon: Girişlerin toplam etkisi = tek tek etkilerin toplamı.

ULA: Eşit aralıklı doğrusal dizi.

Yönlendirme vektörü (a): Kaynak yönünün uzaysal imzası.

λ (dalga boyu): λ = c/f. 500 Hz'de 0.68 m.

Beyazlatma: Korelasyonlu gürültüyü bağımsız yapma.

Cauchy–Schwarz: $|u^*v|^2 \leq (u^*u)(v^*v)$. Eşleşmiş filtrenin temeli.

Durağan sinyal: İstatistiksel özellikleri değişmeyen sinyal.

Gauss–Markov: LS'nin BLUE olduğunu belirten teorem.

Izdüşüm: Vektörün alt uzaya dik bileşeni.

Woodbury özdeşliği: Ters matris formülü. MVDR'da kullanılır.

Wiener filtresi: Doğrusal MMSE tahmincisi. R_sx R_xx^{-1} x.

Wirtinger kalkülüsü: Karmaşık değişkenler için türev alma yöntemi. LS türetiminde kullanılır.

Varyans: Rastgele değişkenin yayılma ölçüsü. Gürültü gücü ile ilişkilidir.

Yanlılık (bias): Tahmincinin beklenen değeri ile gerçek değer arasındaki fark.

Yıkıcı girişim: Farklı fazlardaki sinyallerin birbirini söndürmesi.

Yapıcı girişim: Aynı fazlardaki sinyallerin birbirini güçlendirmesi.

Zaman gecikmesi: Sesin mikrofona ulaşma süresi: $\tau = d \sin\theta / c$.

Kaynaklar

Aitken, A. C. (1935). On least squares and linear combinations of observations. *Proceedings of the Royal Society of Edinburgh, 55*, 42–48.

Balanis, C. A. (2016). *Antenna theory* (4th ed.). Wiley.

Benesty, J., Chen, J., & Huang, Y. (2008). *Microphone array signal processing*. Springer.

Björck, Å. (1996). *Numerical methods for least squares problems*. SIAM.

Brandstein, M., & Ward, D. (Eds.). (2001). *Microphone arrays*. Springer.

Capon, J. (1969). High-resolution frequency-wavenumber spectrum analysis. *Proc. IEEE, 57*(8), 1408–1418.

Cooley, J. W., & Tukey, J. W. (1965). An algorithm for the machine calculation of complex Fourier series. *Math. Comp., 19*(90), 297–301.

Gauss, C. F. (1809). *Theoria motus corporum coelestium*. Perthes.

Golub, G. H., & Van Loan, C. F. (2013). *Matrix computations* (4th ed.). JHU Press.

Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The elements of statistical learning* (2nd ed.). Springer.

Haykin, S. (2014). *Adaptive filter theory* (5th ed.). Pearson.

Hoerl, A. E., & Kennard, R. W. (1970). Ridge regression. *Technometrics, 12*(1), 55–67.

Johnson, D. H., & Dudgeon, D. E. (1993). *Array signal processing*. Prentice Hall.

Kailath, T., Sayed, A. H., & Hassibi, B. (2000). *Linear estimation*. Prentice Hall.

Kay, S. M. (1993). *Fundamentals of statistical signal processing, Vol. I*. Prentice Hall.

Makhoul, J. (1975). Linear prediction: A tutorial review. *Proc. IEEE, 63*(4), 561–580.

Moore, E. H. (1920). On the reciprocal of the general algebraic matrix. *Bull. AMS, 26*, 394–395.

North, D. O. (1943). Signal/noise discrimination. *RCA Report PTR-6C*.

Oppenheim, A. V., & Schafer, R. W. (2010). *Discrete-time signal processing* (3rd ed.). Prentice Hall.

Penrose, R. (1955). A generalized inverse for matrices. *Proc. Cambridge Phil. Soc., 51*(3), 406–413.

Schmidt, R. O. (1986). Multiple emitter location. *IEEE Trans. AP, 34*(3), 276–280.

Tikhonov, A. N. (1963). Solution of incorrectly formulated problems. *Soviet Math. Doklady, 4*, 1035–1038.

Turin, G. L. (1960). An introduction to matched filters. *IRE Trans. IT, 6*(3), 311–329.

Van Trees, H. L. (2002). *Optimum array processing*. Wiley.

Van Veen, B. D., & Buckley, K. M. (1988). Beamforming. *IEEE ASSP Mag., 5*(2), 4–24.

Wiener, N. (1949). *Extrapolation, interpolation, and smoothing*. MIT Press.

BÖLÜM 2

KAN DAĞITIM AĞLARINDA ROTA OPTİMİZASYONUNA YUSUFÇUK VE KIZIL TİLKİ ALGORİTMALARININ UYGULANMASI VE PERFORMANS ANALİZLERİ

Şükran KONCA[1]
Bayram KÖSE[2]
Ali Mert SAĞLAM[3]
Semra ATALAN[4]

Giriş

En kısa yol bulma, rota planlama ve kaynak dağılımı gibi problemler, optimizasyonun temel uygulama alanları arasında yer almaktadır. Bu problemlerden biri olan Gezgin Satıcı Problemi

[1] Profesör, İzmir Bakırçay Üniversitesi, Mühendislik ve Mimarlık Fakültesi, Temel Bilimler Bölümü, Orcid: *0000-0003-4019-958X*
[2] Doktor Öğretim Üyesi, İzmir Bakırçay Üniversitesi, Mühendislik ve Mimarlık Fakültesi, Elektrik Elektronik Mühendisliği Bölümü, Orcid: 0000-0003-0256-5921
[3] Öğrenci, İzmir Bakırçay Üniversitesi Lisansüstü Eğitim Enstitüsü, Akıllı Sistemler Mühendisliği Tezli Yükseklisans Programı, Orcid: 0009-0003-4988-6164
[4] Öğrenci, Bitlis Eren Üniversitesi Lisansüstü Eğitim Enstitüsü, İstatistik Tezli Yükseklisans Programı, Uygulamalı İstatistik Anabilim Dalı, semraatalann@gmail.com, ORCID: 0000-0001-6343-5448

(Traveling Salesman Problem - TSP), belirli şehirleri yalnızca bir kez ziyaret ederek en kısa rotayı bulmayı amaçlar. TSP'nin çözümü; lojistik şirketlerinin dağıtım maliyetlerini azaltması, akıllı şehir uygulamalarında rota verimliliği sağlaması ve robotik sistemlerin görev planlamasında kritik rol oynar.

NP-zor kategorisinde yer alan TSP, çözüm uzayının problem boyutuyla birlikte üstel biçimde genişlemesi nedeniyle klasik deterministik yöntemlerle pratik zamanlarda çözülememektedir. Bu çalışmada, TSP'nin çözümü için doğadan esinlenen iki meta-sezgisel algoritma olan Kızıl Tilki Optimizasyonu (Red Fox Optimization - RFO) ve Yusufçuk Algoritması (Dragonfly Algorithm - DA) incelenmiştir. Bu algoritmalar, doğadaki canlıların hayatta kalma stratejilerini matematiksel modellerle taklit ederek, avlanma ve sürü davranışlarından ilham alarak karmaşık çözüm uzaylarında daha etkili bir arama ve yakınsama yeteneği sunmaları nedeniyle alternatif optimizasyon yaklaşımları olarak ön plana çıkmaktadır.

Araştırma kapsamında, İzmir ilinde bulunan Kızılay Kan Merkezi'nden özel hastanelere gerçekleştirilen kan sevkiyatlarının rota optimizasyonuna yönelik gerçek dünya tabanlı bir problem ele alınmış ve söz konusu problem TSP modeli altında yapılandırılmıştır. Çalışmada, İzmir şehir sınırları içerisinde yer alan 20 hastanenin coğrafi koordinatları kullanılarak her iki algoritma Python programlama dili ile aynı başlangıç parametreleri altında çalıştırılmıştır. Elde edilen rotalar çözüm kalitesi, yakınsama davranışı ve hesaplama süresi bakımından kapsamlı biçimde analiz edilerek performansları karşılaştırılmıştır.

Deneysel sonuçlar, Yusufçuk Algoritması'nın güçlü küresel arama yeteneği sayesinde çözüm uzayının daha geniş bölümünü etkin biçimde taradığını gösterirken; Kızıl Tilki Optimizasyonu'nun daha hızlı yakınsama özellikleriyle hesaplama süresi açısından avantaj sağladığını ortaya koymuştur. Bununla birlikte, her iki algoritma da

rota optimizasyonu bağlamında uygulanabilir ve etkili çözüm yaklaşımı sunmaktadır.

Genel olarak çalışma, meta-sezgisel yöntemlerin TSP gibi karmaşık optimizasyon problemlerine uygulanmasına yönelik kapsamlı bir yöntemsel çerçeve sunmakta olup; özellikle sağlık lojistiği gibi zaman ve kaynak yönetiminin kritik olduğu alanlarda karar vericilere önemli katkılar sağlayabilecek niteliktedir. Ayrıca geliştirilen yaklaşım, benzer yapıya sahip diğer lojistik ve dağıtım problemlerine de uyarlanabilir özelliktedir.

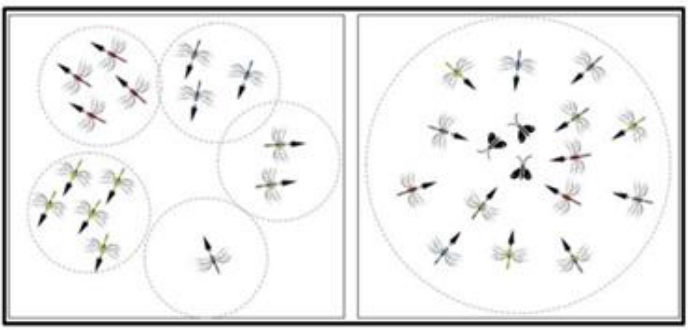
Materyal ve Yöntem

Bu çalışmada, gezgin satıcı probleminin çözümü için Yusufçuk ve Kızıl Tilki algoritmaları kullanılarak elde edilen sonuçlar kıyaslanmıştır. Gezgin satıcı probleminin Yusufçuk algoritması ve Kızıl Tilki algoritması ile çözümünde Python kullanılmıştır. Araştırmada, İzmir şehri içerisinde belirlenen 20 gerçek hastane koordinatı üzerinden algoritmalar uygulanarak ve elde edilen rotalar karşılaştırılarak çözüm kalitesi ve hesaplama süresi bakımından her iki algoritma kıyaslanarak değerlendirilmiştir.

Yusufçuk Algoritması

Analitik olarak çözülmesi zor problemlerde optimizasyon algoritmalarına başvurulur. Yusufçuk Algoritması (DA), optimizasyon problemlerinin çözümünde kullanılan popüler ve yeni sezgisel algoritmalardan biridir. Bu algoritma, 2016'da Mirjalili tarafından geliştirilmiş sürü tabanlı bir optimizasyon algoritmasıdır. Görüntü işleme, robotik, medikal, mühendislik ve daha birçok alanda kullanılmaktadır. Birçok optimizasyon algoritması doğadan esinlenerek geliştirilmektedir. Benzer şekilde Yusufçuk Algoritmasının geliştirilmesinde, yusufçukların doğada sürü

halindeki statik ve dinamik davranışları dikkate alınmıştır. Yusufçuklar iki amaç doğrultusunda sürü halinde uçarlar: avlanma ve göç etme. Yusufçukların bu davranışları, optimizasyondaki keşif ve sömürü olarak adlandırılan iki temel aşamaya benzetilebilir. Şekil 1'de sol tarafta gösterildiği gibi, küçük gruplar halinde yiyecek aramak (avlanma) için küçük bir alanda ileri-geri uçan sürü, statik sürü olarak adlandırılır. Şekil 1'de sağ tarafta gösterildiği gibi, uzak mesafelere göç etmek için tek bir yönde hareket eden çok sayıda yusufçuğun oluşturduğu sürü ise dinamik sürü olarak adlandırılır (Aygün, 2023).



Şekil 1 Statik ve dinamik sürü

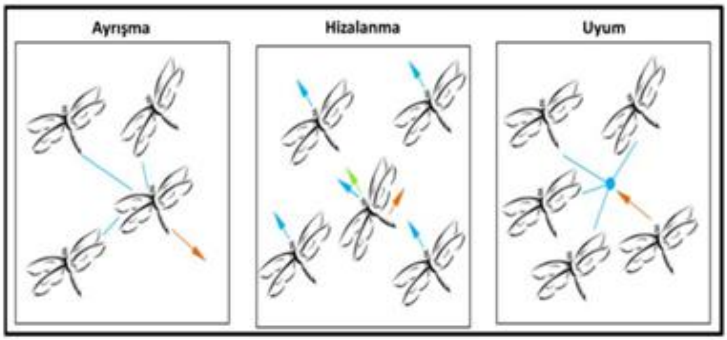
Yusufçuk Algoritmasının Aşamaları

Reynolds'a göre, sürülerin davranışları üç temel prensiple açıklanabilir (Reynolds, 1987; Aygün, 2023):

• Ayrışma: Bireylerin ortamdaki diğer bireylerle statik çarpışmadan kaçınmasını ifade eder.

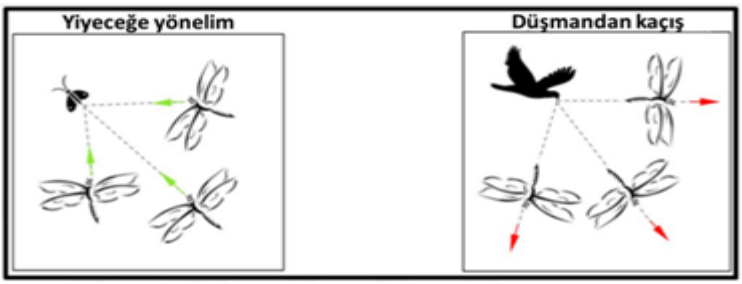
• Hizalanma: Bireylerin ortamdaki diğer bireylerle hız eşleşmesini ifade eder.

Uyum: Bireylerin komşu bireylerin ağırlık merkezine doğru yönelimini ifade eder. Bu üç temel prensip Şekil 2'de gösterilmektedir (Aygün, 2023).



Şekil 2 Sürüdeki bireylerin 3 temel davranışı

Sürünün ana hedefi hayatta kalmaktır. Bu sebeple sürüdeki tüm bireyler yaşamını sürdürebilmek için bir taraftan yiyecek aramalı, diğer taraftan düşmanlarından kaçınmalıdır. Sürüdeki bireylerin bu iki davranışı Şekil 3'te gösterilmektedir.



Şekil 3 Sürüdeki bireylerin hayatta kalması için yaptığı 2 zorunlu davranışı

Yusufçuk algoritmasında bu beş davranışın her biri aşağıdaki gibi matematiksel olarak modellenmektedir.

Ayrışma davranışı Eşitlik 1'de verildiği gibi modellenir.

$$S_i = -\sum_{j=1}^{N} X - X_j \quad (1)$$

Hizalanma davranışı Eşitlik 2'de verildiği gibi modellenir.

$$A_i = \frac{\sum_{j=1}^{N} V_j}{N} \quad (2)$$

Uyum davranışı Eşitlik 3'te verildiği gibi modellenir.

$$C_i = \frac{\sum_{j=1}^{N} X_j}{N} - X \quad (3)$$

Bu denklemlerdeki X mevcut bireyin pozisyonunu, Xj, j. komşu bireyin pozisyonunu, N komşu bireylerin sayısını ve Vj, j. komşu bireyin hızını ifade eder.

Yiyeceğe yönelim ve düşmandan kaçış davranışları sırasıyla Denklem 4'te ve Denklem 5'te verildiği gibi modellenir.

$$F_i = X^+ - X \quad (4)$$

$$E_i = X^- + X \quad (5)$$

Bu denklemlerdeki X mevcut bireyin pozisyonunu, X^+ yiyeceğin pozisyonunu, X^- ise düşmanın pozisyonunu ifade eder.

Bir arama uzayındaki yapay yusufçukların pozisyonunu güncellemek ve onların hareketlerini simüle etmek için iki vektör dikkate alınır: Adım vektörü (ΔX) ve Pozisyon vektörü (X). Hız vektörü olarak da düşünebileceğimiz adım vektörü, yusufçukların hareket yönünü gösterir. Adım vektörü ve pozisyon vektörü sırasıyla aşağıdaki gibi güncellenir.

$$\Delta X_{t+1} = (sS_i + aA_i + cC_i + fF_i + eE_i) + w\Delta X_t \quad (6)$$

$$X_{t+1} = X_t + \Delta X_{t+1} \quad (7)$$

Bu denklemlerdeki s ayrışma ağırlık katsayısını, Si, i. bireyin ayrışmasını, a hizalanma ağırlık katsayısını, Ai, i. bireyin hizalanmasını, c uyum ağırlık katsayısını, Ci, i. bireyin uyumunu, f yiyeceğe yönelim ağırlık katsayısını, Fi, i. bireyin yiyeceğe yönelimini, e düşmandan kaçış ağırlık katsayısını, Ei, i. bireyin düşmandan kaçışını, w eylemsizlik katsayısını, t mevcut iterasyon numarasını ifade eder.

Optimizasyon boyunca yapay yusufçukların keşif ve sömürü davranışları bahsedilen ayrışma, hizalanma, uyum, yiyeceğe yönelim ve düşmandan kaçış ağırlık katsayıları tarafından belirlenir.

Statik sürüde yiyecek aramak için uyum yüksek iken, hizalanma çok düşüktür.

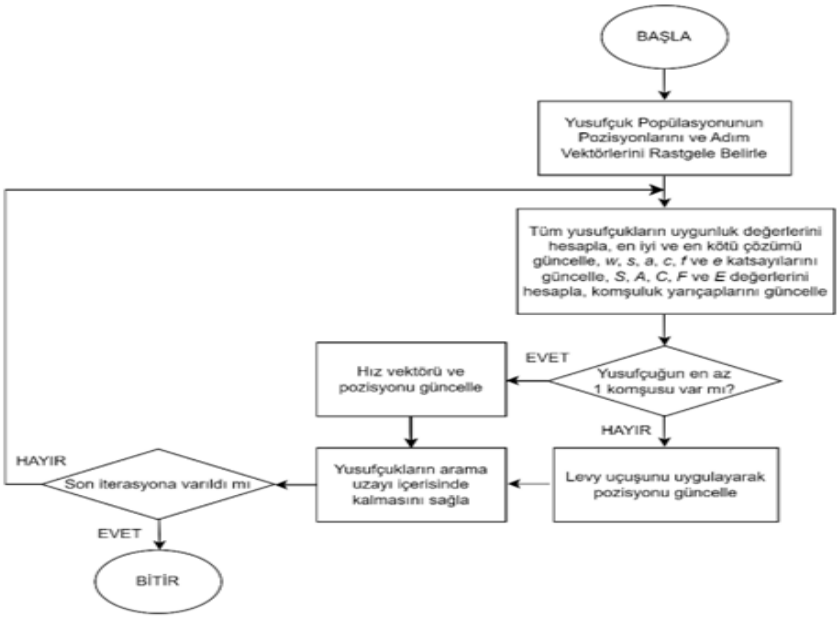
Dinamik sürüde ise yusufçuklar uçuşlarını hizalama eğilimi gösterirler. Bu sebeple Yusufçuk algoritmasında keşif sürecinde uyum ağırlık katsayısı düşük, hizalanma ağırlık katsayısı yüksek atanırken, sömürü sürecinde uyum ağırlık katsayısı yüksek, hizalanma ağırlık katsayısı düşük atanır (Aygün, 2023).

Yusufçuk Algoritmasının Akış Diyagramı

Tablo 1'de Yusufçuk algoritmasının sözde kodu verilirken, Şekil 4'te ise Yusufçuk algoritmasının akış diyagramı verilmektedir (Aygün, 2023).

Tablo 1 Yusufçuk algoritmasının sözde kodu

Arama uzayında rastgele bir yusufçuk popülasyonu oluştur *X_i (i=1,2,...,n).*
Belirlenen sınır değerleri içinde rastgele adım vektörü oluştur ΔX_i *(i=1,2,...,n).*
While (Birinci iterayondan son iterasyona kadar devam et)
Hedef fonksiyonuna göre bütün yusufçukların uygunluk değerini hesapla
En iyi çözümü (yiyeceğin pozisyonu) ve en kötü çözümü (düşmanın pozisyonu)
Güncelle
Ağırlık katsayılarını güncelle (*w,s,a,c,f* ve *e*)
Eşitlik 1-5 kullanarak *S, A, C, F* ve *E* değerlerini hesapla
Komşuluk yarıçapını güncelle
if (Yusufçuğa komşu en az bir yusufçuk varsa)
Eşitlik 6 kullanarak Adım vektörünü güncelle
Eşitlik 7 kullanarak Pozisyon vektörünü güncelle
else
Eşitlik 8 kullanarak Pozisyon vektörünü güncelle
end if
Yusufçukların arama uzayı sınırlarında kalmasını sağla
end while



Şekil 4 Yusufçuk algoritmasının akış diyagramı

```python
def yusufcuk_algoritmasi(mesafe_matrisi, iterasyonlar=iterasyon):
    n = len(mesafe_matrisi)
    popülasyon_boyutu = 20
    popülasyon = [np.random.permutation(n) for _ in range(popülasyon_boyutu)]
    en_iyi_rota = popülasyon[0].copy()
    en_iyi_mesafe = toplam_mesafe(en_iyi_rota, mesafe_matrisi)

    for _ in range(iterasyonlar):
        # Her yusufçuk için yeni pozisyon hesapla
        for i in range(popülasyon_boyutu):
            mevcut = popülasyon[i].copy()
            # Rastgele iki nokta seç ve değiştir
            i1, i2 = random.sample(range(n), 2)
            mevcut[i1], mevcut[i2] = mevcut[i2], mevcut[i1]

            # Yerel arama: 2-opt değişimi
            if random.random() < 0.75:  # %75 olasılıkla yerel arama yap
                i1, i2 = sorted(random.sample(range(n), 2))
                mevcut[i1:i2+1] = mevcut[i1:i2+1][::-1]

            mevcut_mesafe = toplam_mesafe(mevcut, mesafe_matrisi)
            if mevcut_mesafe < toplam_mesafe(popülasyon[i], mesafe_matrisi):
                popülasyon[i] = mevcut.copy()
                if mevcut_mesafe < en_iyi_mesafe:
                    en_iyi_mesafe = mevcut_mesafe
                    en_iyi_rota = mevcut.copy()

    return en_iyi_rota, en_iyi_mesafe
```

Şekil 5 Yusufçuk algoritması Python kodu

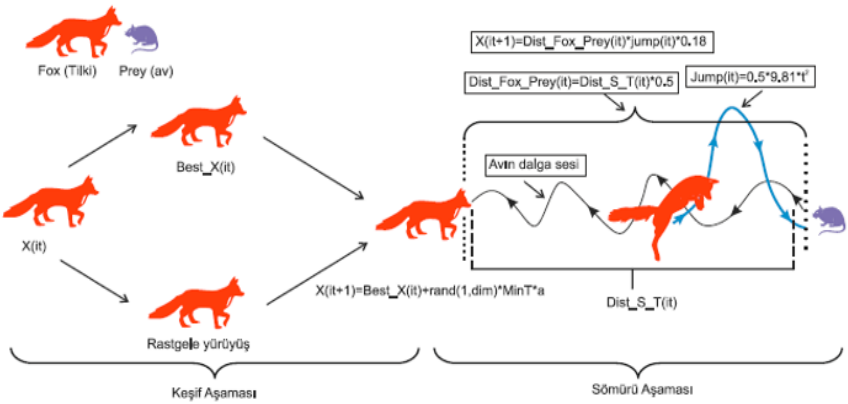
Kızıl Tilki Optimizasyon Algoritması

Doğadaki canlıların yaşayış biçimleri meta-sezgisel optimizasyon yöntemlerine ilham kaynağı olmaktadır. Doğada sürü halinde yaşayan canlıların sergiledikleri sezgisel hareketler, avlanma şekilleri ve yaşayış tarzları matematiksel olarak modellenerek çeşitli problemlerin çözümü için farklı optimizasyon algoritmaları geliştirilmiştir. (Yaylacı, Yılmaz, Özdeş, 2022). Metasezgisel yöntemlerin avantajları arasında; analitik yöntemlerin yetersiz kaldığı karmaşık ve çok boyutlu problemlere uygulanabilirliği; lokal optimuma takılmadan global çözümü bulma potansiyeline sahip olması; stokastik bir yapıya sahip oluşundan, farklı çalıştırmalarda farklı çözümler üretebilmesi gelir. Bu durum, problemin farklı yönlerini keşfetmeye ve en iyi çözüme ulaşma şansını artırmaya yardımcı olabilir. Kızıl Tilki Algoritması, bu çalışmada ele alınan yeni bir metasezgisel yöntemdir. Bu yöntem, kızıl tilkilerin avlanma ve sürü içi davranışlarından ilham alarak tasarlanmıştır. Algoritma, avcı-av ilişkisi ve sürü içi hiyerarşi gibi kavramları kullanarak optimizasyon problemlerine çözüm bulmayı amaçlamaktadır.

Kızıl Tilki Algoritması, doğadaki karmaşık davranışlardan ilham alarak tasarlanmıştır. Bu durum, algoritmaya sağlamlık ve esneklik kazandırır. Kızıl Tilki Algoritması, avcı-av ilişkisi ve sürü içi hiyerarşi gibi kavramları kullanarak arama alanını etkin bir şekilde tarayabilir. Kızıl Tilki Algoritması, lokal optimuma takılmadan global çözümü bulma potansiyeline sahiptir.

Kızıl Tilki Optimizasyon (RFO) Algoritması Kızıl tilkilerin popülasyonu, belirli bölgelerde yaşayan ve göçebe bir hayat süren bireylerden oluşur. Her sürü, alfa çiftin hiyerarşisi altında tek bir bölgeyi paylaşır. Gençler büyüdüklerinde, başka bir bölgeyi ele geçirme şansları yüksekse sürüden ayrılıp kendi sürülerini kurabilirler. Aksi takdirde, ailede kalırlar ve bir gün ebeveynlerinden avlanma alanını devralırlar. Kırmızı tilki, hem evcil hem de yaban hayvanları olan küçük hayvanların etkili bir avcısıdır. Tilkiler, bölgeyi dolaşırken her fırsatta yiyecek ararlar, avlarına sinsice

yaklaşırlar ve etkili bir saldırı için yeterince yaklaşana kadar saklanırlar. Bu algoritma, yiyecek arayışında tilkilerin avları uzaktayken bölgeyi keşfetmelerini küresel arama olarak modellemiştir. İkinci aşamada, avlanmadan önce mümkün olduğunca yaklaşmak için habitatı dolaşmak yerel arama olarak modellenmiştir.



Şekil 6 Kızıl tilki avlanma davranışı: keşif ve sömürü (Mohammed ve Rashid, 2023).

Temel Algoritma Önermesinde her iterasyonda, bireylerin sabit sayıda tilkiden oluştuğu varsayılır. Her biri, n koordinatlı bir nokta olarak temsil edilir. Her tilkinin iterasyon t'deki gösterimiyle ayırt edilir, burada i popülasyondaki tilkinin numarasını ve j çözüm uzayının boyutlarına göre koordinatı temsil eder. Tilkilerin, optimum değerler için kriter fonksiyonunda çözüm aradığı varsayılır.

Yiyecek Arayışında — Küresel Arama Aşaması: Bir sürüde, her tilkinin tüm aile üyelerinin hayatta kalması için önemli bir rol oynaması gerekir. Yerel habitatlarda yiyecek yoksa veya diğer bölgeleri keşfetmek için, sürü üyeleri uzak destinasyonlara seyahat ederler. Bu keşifte elde ettikleri bilgileri aileyle paylaşırlar.

Yerel Habitatı Dolaşma — Yerel Arama Aşaması: Kırmızı tilki, potansiyel avları arayarak kendi bölgesini dolaşır. Mümkün olan bir av gördüğünde, tilki fark edilmeden mümkün olduğunca yaklaşmak için sessizce yaklaşmaya başlar. Bu nedenle, avı kandırmak ve avın kendisiyle ilgilenmediğine ikna etmek için avın etrafında dolaşır ve aldatır.

Üreme ve Sürüden Ayrılma: Doğada, kırmızı tilki birçok tehlikeyle karşı karşıya kalır. Yerel habitat alanında yiyecek olmayabilir, bu nedenle başka bir yere taşınmak gerekebilir. Başka bir tehlike insanlardan gelir. Eğer evcil hayvan popülasyonunda büyük zararlar olursa, insanlar tilkiyi avlayabilir.

Bu davranışları modellemek için, her iterasyonda kriter fonksiyon değerine göre popülasyonun en kötü %5'ini seçeriz. Bu, sürüden ayrılan veya avcılar tarafından vurulan tilkiler olarak varsayılır. Popülasyondaki birey sayısını sabit tutmak için, alfa çift tarafından kurulan habitat bölgesi kullanılarak onları yeni bireylerle değiştiririz.

Sonuçta önerilen yöntem, her iterasyonda en uygun bireyi seçerek ve sonraki iterasyonlarda en iyi sonucu geliştirerek sıralı bir dizi (x^*) oluşturur. Optimizasyon, sonraki iterasyonlarda tekrarlanır ve en iyi sonuç iyileştirilir.

Kızıl Tilki optimizasyon yönteminde, aşağıdaki parametreler alınarak,

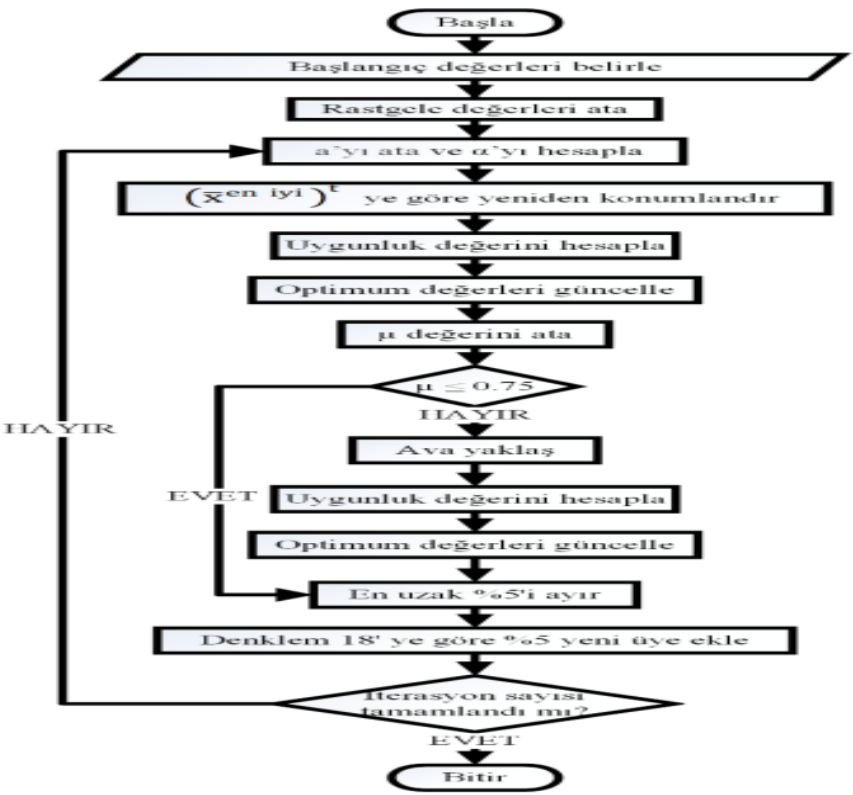
```
% Parametreler
numFoxes = 40; % Tilki sayısı
numIterations = 100; % Maksimum iterasyon sayısı
lb = [0, 0]; % Alt sınırlar
ub = [15, 15]; % Üst sınırlar
nVar = length(ub);% boyut
alpha_fraction =0.05; %En kötü %5 tilkileri belirlemek için
alpha_pair_threshold =0.44; %Alfa çifti üreme eşik değeri
```

- Başlangıç pozisyonlarını oluşturma

- Başlangıç uygunluk değerlerini hesaplama
- Global Arama (Yemek Arama)/ Keşif
- Lokal Arama (Lokal Habitat) /Sömürü
- Sürüden Ayrılma ve Sürüye Katılma
- En iyi tilkiyi güncelle
- Sonuçları yazdır

adımları izlenmiştir.

Kızıl tilki algoritmasına ait akış diyagramı Şekil 7 ile ifade edildiği gibidir (Yaylacı, Yılmaz, Özdeş, 2022).



Şekil 7 Kızıl tilki algoritması akış şeması

```python
def kizil_tilki_algoritmasi(mesafe_matrisi, iterasyonlar=iterasyon):
    n = len(mesafe_matrisi)
    tilki_sayisi = 40  # Popülasyon büyüklüğü
    alpha_fraction = 0.05  # En kötü %5 tilkileri belirlemek için
    alpha_pair_threshold = 0.44  # Alfa çifti üreme eşik değeri

    # Başlangıç popülasyonunu oluştur (ilk nokta sabit)
    tilkiler = [np.concatenate(([0], np.random.permutation(n-1) + 1)) for _ in range(tilki_sayisi)]
    uygunluklar = np.array([toplam_mesafe(tilki, mesafe_matrisi) for tilki in tilkiler])

    # En iyi tilkiyi bul
    en_iyi_tilki_idx = np.argmin(uygunluklar)
    en_iyi_tilki = tilkiler[en_iyi_tilki_idx].copy()
    en_iyi_mesafe = uygunluklar[en_iyi_tilki_idx]

    for iterasyon in range(iterasyonlar):
        # Her tilki için yeni pozisyon hesapla
        for i in range(tilki_sayisi):
            mevcut_tilki = tilkiler[i].copy()

            # Global Arama (Yemek Arama) / Keşif
            if random.random() < 0.5:
                # Rastgele iki nokta seç (ilk nokta hariç)
                i1, i2 = random.sample(range(1, n), 2)
                mevcut_tilki[i1], mevcut_tilki[i2] = mevcut_tilki[i2], mevcut_tilki[i1]

            # Lokal Arama (Lokal Habitat) / Sömürü
            else:
                # 2-opt değişimi (ilk nokta hariç)
                i1, i2 = sorted(random.sample(range(1, n), 2))
                mevcut_tilki[i1:i2+1] = mevcut_tilki[i1:i2+1][::-1]

            # Yeni uygunluk değerini hesapla
            yeni_mesafe = toplam_mesafe(mevcut_tilki, mesafe_matrisi)

            # Eğer yeni pozisyon daha iyiyse, güncelle
            if yeni_mesafe < uygunluklar[i]:
                tilkiler[i] = mevcut_tilki.copy()
                uygunluklar[i] = yeni_mesafe

                # En iyi tilkiyi güncelle
                if yeni_mesafe < en_iyi_mesafe:
                    en_iyi_mesafe = yeni_mesafe
                    en_iyi_tilki = mevcut_tilki.copy()

        # Sürüden Ayrılma ve Sürüye Katılma
        if iterasyon % 10 == 0:  # Her 10 iterasyonda bir
            # En kötü tilkileri belirle
            alpha_sayisi = int(tilki_sayisi * alpha_fraction)
            en_kotu_indeksler = np.argsort(uygunluklar)[-alpha_sayisi:]

            # En kötü tilkileri yeniden başlat
            for idx in en_kotu_indeksler:
                if random.random() < alpha_pair_threshold:
                    # Yeni rastgele rota oluştur (ilk nokta sabit)
                    tilkiler[idx] = np.concatenate(([0], np.random.permutation(n-1) + 1))
                    uygunluklar[idx] = toplam_mesafe(tilkiler[idx], mesafe_matrisi)

        # İlerleme durumunu yazdır
        if iterasyon % 1000 == 0:
            print(f"İterasyon {iterasyon}: En iyi mesafe = {en_iyi_mesafe:.2f}")
```

Şekil 8 Kızıl tilki algoritması Python kodu

Gezgin Satıcı Problemi

Gezgin Satıcı Problemi (Travelling Salesman Problem-TSP) bir satıcının belirli bir kasabadan başlayarak, satış bölgesinde yer alan tüm kasabaları sadece bir kez ziyaret etmek koşulu ile tekrar başlangıç kasabasına dönmesini ifade eder. Satıcının bu turu kapalı bir çevrimdir ve problem olası ziyaret sıralamalarının tümünü ifade eden çözüm uzayındaki en kısa turu veren çözümü elde etmektir. TSP için bir çok farklı problem tipi tanımlanmıştır. TSP tanımlanması ve anlatılması kolay, ancak çözümü oldukça zor bir problemdir. Küçük boyutlu problemler kesin matematiksel yöntemlerle çözülebilirken, çok büyük problemlerin kesin matematiksel yöntemlerle çözümü mümkün değildir. TSP bilimsel yazında NP-zor sınıfında yer alan bir problem olarak belirli hale gelmiştir. Kombinatoryal optimizasyon problemleri sınıfında yer alan TSP için literatürün büyük çoğunluğu sezgisel ve metasezgisel yaklaşımlardan oluşmaktadır. Sezgisel ve metasezgisellerin yoğun şekilde kullanılması bir tesadüf değildir. Çünkü ancak bu yaklaşımların kullanımıyla optimal ve/veya optimale yakın çözümlere kabul edilebilir sürelerde ulaşılabilmektedir (Karagül, 2019b).

TSP, iki yüzyıl öncesinden beri yaygın olarak kullanılan kombinatoryal optimizasyon problemlerinden biridir. Eğer bir harita bir dizi şehir içeriyorsa ve her iki şehir arasındaki mesafe önceden biliniyorsa. Ve bir satıcı bu kasabalar arasında belirli bir kasabadan başlayıp diğer tüm kasabalardan geçerek bir tur yapmak isterse. Her şehir bir kez ziyaret edilmeli (Hamilton döngüsü) ve toplam maliyeti en az olan ilk şehre geri dönülmelidir. TSP'nin üstesinden gelmenin zorluğu, kasaba sayısı arttığında ortaya çıkar; kasaba sayısının artması, en iyi çözümleri (minimum toplam mesafeye sahip çözüm) bulmak için daha fazla zamana ihtiyaç duyulması anlamına gelir

(Hammouri, Abu Samra, Al-Betar, Raid Khalil, Alasmer, Kanan, 2018).

TSP, *G=(V,E)* grafiği olarak gösterilebilir; burada *V*, şehirleri temsil eden bir köşeler kümesidir ve *E*, herhangi iki şehir arasındaki yolu temsil eden bir kenarlar kümesidir. Aşağıdaki denklem TSP'nin amaç fonksiyonunu göstermektedir:

$$F(T) = Min(\sum_{i=1}^{k} D_{i,i+1} + D_{k,1}) \quad (1)$$

Burada *K* köşe sayısını, *D* mesafeyi, *T* turu ve *F(T)* turun toplam mesafesini temsil eder. Son olarak, TSP'nin temel amacı, bu problemin diğer önceki koşullarını da göz önünde bulundurarak mümkün olan en kısa maliyeti bulmaktır. Özellikle problemin boyutu büyük olduğunda TSP'nin en iyi çözümünü makul bir süre içinde bulmak için kesin yöntemler kullanmanın zorluğundan bahsetmek gerekir. Tablo 2, şehir sayısı arttığında arama uzayının nasıl genişlediğini göstermektedir, arama uzayının boyutunun *n*'nin faktöriyeli olduğuna dikkat edin. Bu nedenle meta-sezgisel yöntemler, bu tür problemlerin üstesinden gelmek için tercih edilir. Meta sezgisel yöntemler, aşağıdakiler de dahil olmak üzere farklı problemlerin üstesinden gelmede başarısını kanıtlamıştır TSP (Hammouri, Abu Samra, Al-Betar, Raid Khalil, Alasmer, Kanan, 2018).

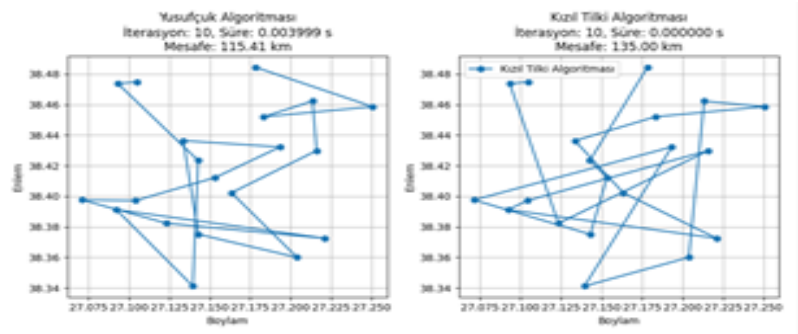
Tablo 2 Şehir sayısı ve arama uzayı büyüklüğü

Şehir sayısı	Arama uzayı büyüklüğü
6	720
10	3.6288×10^{6}
50	$3.04140932 \times 10^{64}$
75	$2.480914081 \times 10^{109}$

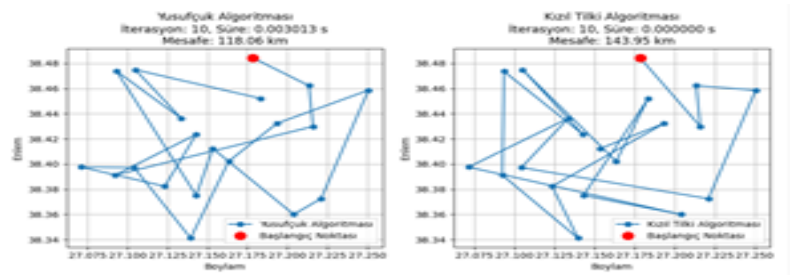
Birçok araştırmacı, Gezgin Satıcı Problemi'ni (TSP) farklı meta-sezgisel yöntemler kullanarak ele almıştır. Bu yöntemler, yalnızca problemi çözmek için tek başına uygulanabildiği gibi,

çözüm kalitesini artırmak amacıyla diğer tekniklerle birleştirilerek hibrit yapılar hâline de getirilebilmektedir. Ancak tüm bu yaklaşımlar, her zaman en iyi (optimal) çözümü garanti edemez. Bu durum, TSP'yi oldukça zorlu bir problem hâline getirirken, aynı zamanda farklı meta-sezgisel yöntemler arasında güçlü bir rekabet ortamı oluşmasına neden olmaktadır (Hammouri, Abu Samra, Al-Betar, Raid Khalil, Alasmer, Kanan, 2018).

Performans Değerlendirmesi ve Analizi

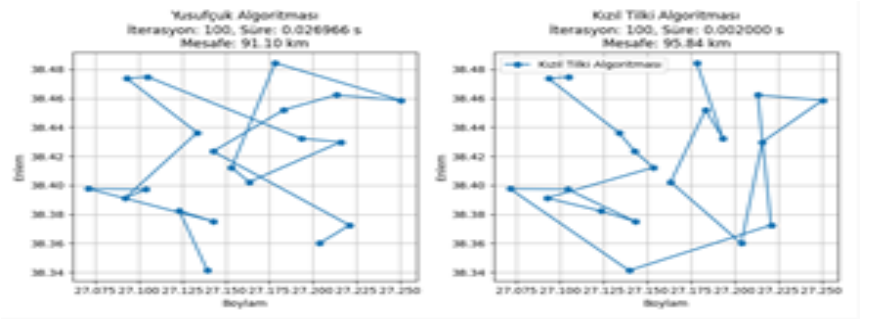


Şekil 9 İterasyon sayısı 10 karşılaştırma

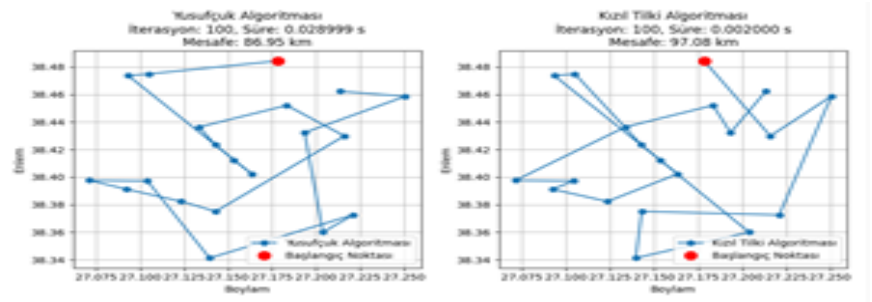


Şekil 10 İterasyon sayısı 10 sabit başlangıç noktalı

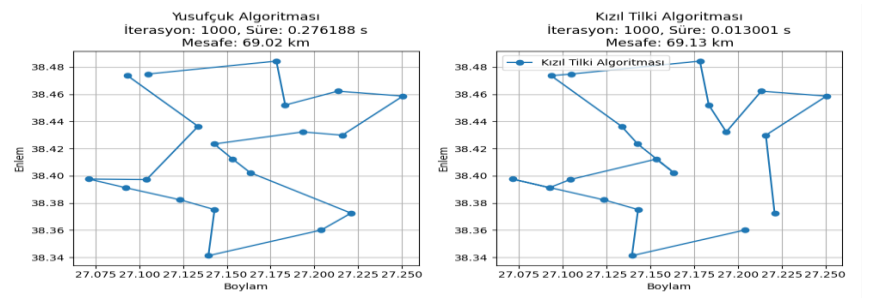
İterasyon sayısı 10 olduğunda, algoritmanın çalışma süresi oldukça kısa ve hesaplama karmaşıklığı düşük seviyededir. Bu durumda işlem adımları hızlıca tamamlanmakta ve performans üzerinde minimal bir yük oluşmaktadır.



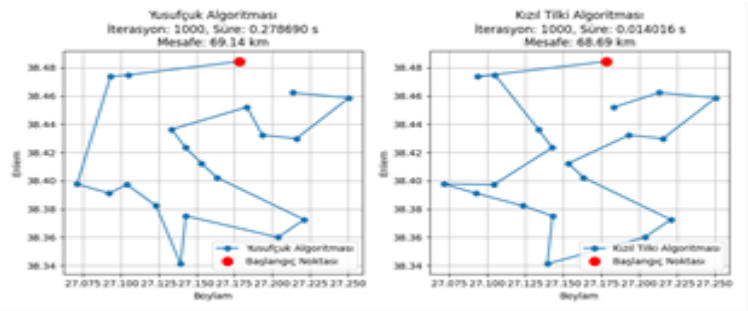
Şekil 11 İterasyon sayısı 100 karşılaştırma



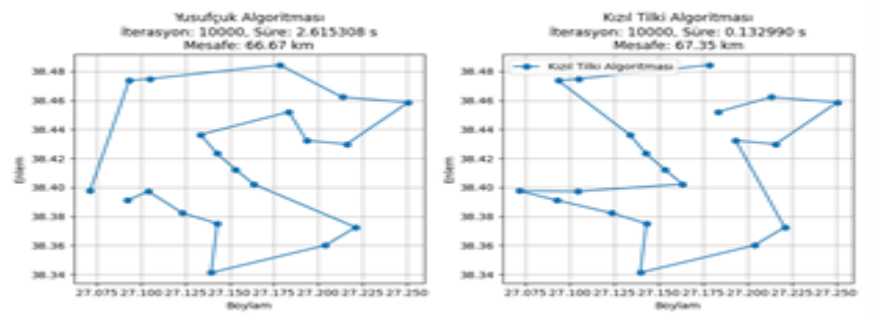
Şekil 12 İterasyon sayısı 100 sabit başlangıç noktalı



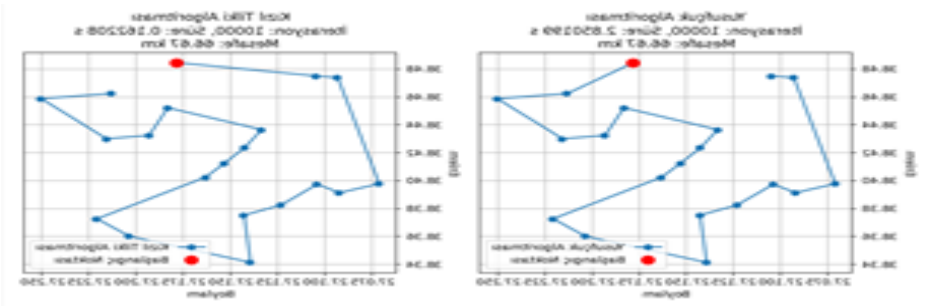
Şekil 13 İterasyon sayısı 1.000 karşılaştırma



Şekil 14 İterasyon sayısı 1.000 sabit başlangıç noktalı



Şekil 15 İterasyon sayısı 10.000 karşılaştırma

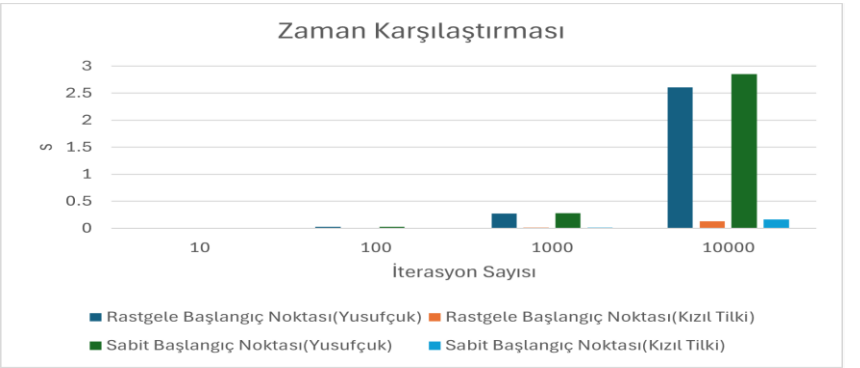


Şekil 16 İterasyon sayısı 10.000 sabit başlangıç noktalı

Yineleme sayısını 10.000'e çıkardığımızda, sistemin çalışma süresi önemli ölçüde uzanır. Bununla birlikte, bu artış, zaman masrafına neden olmasına rağmen elde edilen sonuçların hassasiyeti ve hızı için önemli bir fayda sunmaktadır. Bu, daha uzun sürse bile,

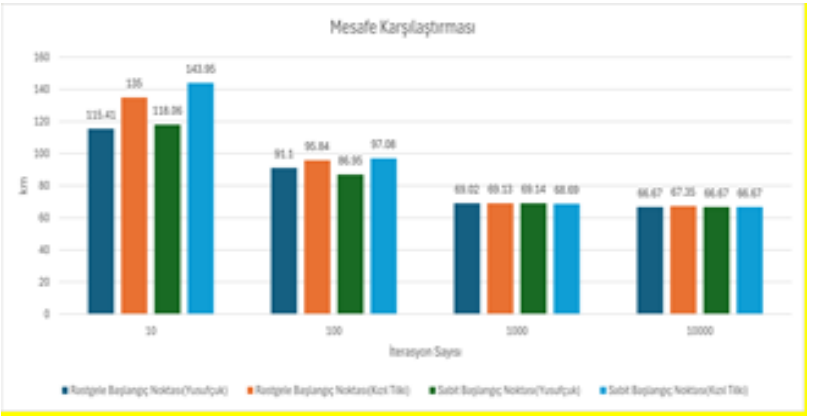
yöntemin daha hızlı ve en iyi rotayı keşfetme olasılığını artıran daha olası seçenekleri kontrol etmede daha iyi bir çekim yapması anlamına gelir. 10.000 denemeden elde edilen sonuçlar en etkili ve en başarılı olanıdır.

Sonuçlar ve Öneriler



Şekil 17 Zamana göre algoritmaların karşılaştırılması

Yapılan deneyler sonucunda, Kızıl Tilki Algoritması (RFO) daha kısa sürede çalışarak zaman açısından avantaj sağlamış, özellikle iterasyon sayısı arttıkça çözüm kalitesini belirgin şekilde iyileştirebilmiştir. Buna karşılık, Yusufçuk Algoritması (DA) daha uzun sürede çalışmasına rağmen genellikle daha kısa rotalar üretmiştir. Bu nedenle, zamanın kritik olduğu uygulamalarda RFO tercih edilebilirken, daha hassas sonuçların gerektiği durumlarda DA algoritması daha uygun bir seçenek olabilir.



Şekil 18 Mesafeye göre algoritmaların karşılaştırılması

Bu deneyde hesaplamalar kuşbakışı yapılmıştır. Mesafe ve süre ilişkisine bakıldığında kızıl tilki algorimasının kullanılması avantajlıdır.

Kaynakça

Aygün, H. (2023). Yusufçuk algoritması, *Teknobilim-2023. Optimizasyon Modelleme ve Yapay Zeka Optimizasyon Algoritmaları*, Efe Akademi Yayınları, Fatih, İstanbul.

Gülcan, H. (2018). *Yusufçuk algoritmasının Brownian hareketiyle iyileştirilmesi*, Mersin Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Mersin.

Hammouri, A. I., Abu Samra, E. T., Al-Betar, M. A., Raid M. Khalil, Alasmer, Z. & Kanan, (2018). M. *A dragonfly algorithm for solving traveling salesman problem*, 2018-8th International Conference on Control System, Computing and Engineering (ICCSCE 2018), 23-25 November 2018, Penang, Malaysia.

Karagül, K. (2019)a. Gezgin satıcı problemi için yeni bir çözüm yaklaşımı: TPORT. *Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi*, 21 (63), 819-832.

Karagül, K. (2019)b. Gezgin satıcı probleminin çözümü için Macar algoritması esaslı yeni bir çözüm yaklaşımı. *Mühendislik Bilimleri ve Tasarım Dergisi*, 7 (3), 561-571.

Katırcıoğlu, F. (2017). Renkli görüntüler için yusufçuk algoritması kullanılarak benzerlik görüntüsüne dayalı eşikleme. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 5, 506-523.

Mirjalili, S. (2016). Dragonfly algorithm: a new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems. *Neural Computing and Applications*, 27, 1053-1073.

Mohammed, H., & Rashid, T. (2023). FOX: a FOX-inspired optimization algorithm. *Applied Intelligence*, 53 (1), 1030-1050.

Tanyıldız, E. & Çelik, A. (2020). Güncel ikili optimizasyon algoritmalarının kısıtsız kıyaslama fonksiyonlarındaki performans karşılaştırmaları. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 32 (2), 369-380.

Yaylacı, E. K., Yılmaz, A. E., & Özdeş. H. N. (2022). Kızıl tilki optimizasyon algoritması ile DA-DA alçaltıcı tip dönüştürücü kontrolör katsayılarının optimizasyonu. *Mühendislik Bilimleri ve Araştırma Dergisi*, 4 (2), 129-140.

BÖLÜM 3

FİNANSAL MODELLEME

GÜLAY SEÇİMTURHAN[1]

Finansal Modelleme Nedir

Finansal modelleme, iş ve yatırım durumlarında sıklıkla kullanılan bir stratejidir. Finansal modellerin yaratılmasının ardındaki temel fikir, belirli bir eylem süreci ile ilgili olabildiğince çok olası senaryo ve sonuçları tanımlamak ve incelemektir. Bu türün modellenmesi çoğu zaman bireylerin ve işletmelerin hangi varlıkların veya diğer yatırımların güvence altına alınacağı ve ayrıca halka ne tür ürünler sunmaya başlayacağı konusunda daha bilinçli kararlar almalarına yardımcı olabilir.

Yatırım ile finansal modelleme, belirli bir yatırımın gelecekteki performansı ile ilişkili tüm olası sonuçları doğru bir şekilde belirlemeye odaklanır. Yatırımcı yalnızca bilinen faktörleri değil, piyasada gelecekteki hareketleri veya siyasi seçimlerin yatırımın değeri üzerindeki etkisini göz önünde bulunduran bir dizi farklı model hazırlar. Bazı modeller ayrıca, bir tür doğal afet meydana gelirse yatırımın ne olacağını tahmin etmek gibi aşırı

[1] Dr.Öğr.Üyesi, Mimar Sinan Güzel Sanatlar Üniversitesi, Fen Edebiyat Fakültesi Matematik Bölümü, İstanbul, Türkiye, gulay.secim@msgsu.edu.tr orcid:0000-0003-4452-666X

faktörlerde içerir. Bu farklı modelleri yaratarak, yatırımcı belirli bir süre için yatırımının güvence altına alınması ve elde tutulması ile ilgili risk hakkında daha iyi fikir edinir. (Çoşkun M., 2016)

Finansal modelleme ayrıca bir şirketin nihayetinde tüketiciyi cezbetmeyen bir ürünün geliştirilmesi, üretilmesi ve tanıtılması için kaynak harcamaktan da kaçınmasına yardımcı olabilir. Tüketici tercihlerinde belirli bir kayma meydana gelirse veya ekonomi bir gerileme geçirirse ne olabileceğini belirlemek için çeşitli modeller kullanarak, o ürünün üretiminde rol alan risk miktarını dikkate almak mümkündür. Modeller, başlangıç maliyetlerini dengelemek için ürünün yeterli gelir elde etmesi olasılığının yüksek olduğunu gösteriyorsa, şirket dikkatini başka bir yöne odaklamayı seçebilir. Aynı zamanda, finansal modelleme başarılı bir sonuç elde etme şansını en üst düzeye çıkarmak için projenin özelliklerini nasıl iyileştireceğiniz konusunda fikirlere yol açabilir. (Çoşkun M., 216, Kaya S., 2020)

Birçok durumda finansal modelleme, opsiyon fiyatlaması, her bir modelle ilişkili sermaye maliyeti, hazırlanan her bir modelin sonucuyla ilgili risk ve başarısızlığa karşı başarı potansiyeli gibi faktörleri dikkate alan matematiksel projeksiyonların oluşturulmasını içerir.

Bu projeksiyonlar için tam konfigürasyon, incelenmekte olan eylemin türüne bağlı olarak değişecektir. Formül, istenen sonucun elde edilmesiyle ilgili doğru ve eksiksiz bilgiler içerdiği sürece, finansal modellemenin üretim ve pazarlama stratejilerini iyileştirmesinin yanı sıra, proje sonucu için makul beklentiler belirleme ihtimali de yüksektir. (Çoşkun M.,2016)

Hisse Senedi Getirisinin Modellenmesi

Yatırım araçlarının getirisi çok genel olarak, ilgili varlığı elde etme zamanı ile değerleme ya da elden çıkarma zamanı arasında yatırımcının servetinde ortaya çıkan net artış şeklinde tanımlanabilir. Her yatırım aracının farklı türde getiriye sahip olması bu temel özelliği değiştirmez. Hisse senedi için getiri, kar payı ve değer artışı olarak iki kısımdan oluşmaktadır. Kar payı periyodik aralıklar ile elde edilirken; değer artışı ise yatırımcının hisse senedini satması ile elde edilmektedir. Bu anlamda hisse senedinin getirisi;

$$r_{it} = \frac{(P_t - P_0)}{(1+i)^t} + \sum_{t=1}^{n} \frac{D_t}{(1+i)^n}$$

formülü ile gösterilir. Formülde P_0: hisse senedinin yatırım dönemi başlangıcındaki değerini, P_t: hisse senedi yatırım dönemi sonundaki değerini, D_t: hisse senedi için her yıl dağıtılacak kar payını ve i faiz oranını göstermektedir. (Çoşkun M., 2016)

Her yıl dağıtılacak kar payının ve yatırım dönemi sonundaki hisse senedinin değeri gelecekte ortaya çıkacağı için risk içermektedir. Bu nedenle beklenen değer ile hisse senedinin getirisinin belirleneceği açıktır. Getirinin beklenen değerini tahmin etmek için gerekli olan olasılıklandırma işlemi, getiri ile ilişkisi olduğu düşünülen değişkenlerin ve bu değişkenler ile getiri arasındaki ilişkinin yönünün ve gücünün belirlenmesiyle mümkün olacaktır. Bu noktadan hareketle, hisse senedinin getirisinin söz konusu değişkenlerin bir bileşkesi olduğu söylenebilir. Değişkenlerin hisse senedi getirisi ile ilişkisini, sabit özelliğe sahip bir ilişki olarak düşünmek ise mümkün değildir. Bunun temel sebebi hisse senedi fiyat hareketinin rassal olmasıdır. Ancak fiyat hareketlerine ilişkin teoriler incelendiğinde bu rassallığın yanında, zaman boyutu da dikkate alınarak tahminlemeyi sağlayabilecek yöntemlerin geliştirilebilmesi, söz konusu değişkenler ile hisse

senedinin getirisi arasındaki ilişkinin önemli ve karar vermeye yardımcı olduğunu göstermektedir. (Çoşkun M., 216, Kaya S., 2020)

Hisse Senedi Fiyat Hareketlerini Açıklayan Teoriler

Hisse senedi fiyat hareketlerini açıklamada kullanılan üç temel strateji bulunmaktadır. İçlerinde en eski olan Dow Teorisi, yatırımcının hisse senedi ile ilgili haberler ışığında verdiği kararların bir sonucu olarak açıklamaktadır. Fiyatın yönünü belirlemeye yönelik olarak oluşturulan stratejiler, Teknik Analizin temelini oluşturmaktadır. Hisse senedi fiyatlarının tamamen rassal hareket ettiği ve bu nedenle bir trend izlemediği temeline dayanan Rassal Yürüyüş Teorisi teknik analize karşıt olarak 1960'lı yılların ikinci yarısında ortaya atılmıştır. Bu iki teorinin gerçeğe uygun olmayan varsayımlarının olması ve yapılan ampirik çalışmalar sonucunda tüm piyasalarda geçerli olmadıklarının anlaşılması sonucu son yıllarda kullanılmaya başlanan bir diğer teori de Kaos Teorisidir. Rassal Yürüyüş teorisinin aksine, hisse senedi fiyat hareketlerini etkileyen değişkenlerin olduğunu fakat bu değişkenler ile ilişkinin ölçülmesinin karmaşık olduğu temeline dayanmaktadır.

Hisse Senetlerinin Özellikleri ve Fiyat Hareketleri

Hisse senedi fiyatlarına ilişkin aşağıdaki beş özelliği incelemenin bir yolu fiyat hareketleri konusunda düşünmektir. Bir hisse senedinin fiyat hareketi belirli bir dönemdeki fiyatın grafiğidir. Hisse senedi fiyat hareketine ilişkin grafikler incelendiğinde beş özelliği yansıttığı görülür.

1. Rassal salınımlı grafiklerdir.

2. Süreklidir ve sıçramalar göstermez.
3. Daima pozitif değerlere sahiptir. Ne kadar düşük değerlere sahip olursa olsun asla sıfır olmaz.
4. Belirli bir zaman noktasında tüm makul düzeydeki grafiklerin ortalaması hisse senedinin başlangıç fiyatından daha yüksektir. Daha uzak noktalarda ortalamanın üzerindedir.
5. Tüm makul düzeydeki grafiklere ait standart sapma zaman ilerledikçe artar.

Lognormal Fiyat Dağılımları ve Geometrik Dağılımlar

$$PeriyodikOrtalama = \mu_{periodic} = \frac{1}{M}\sum_{t=1}^{M} r_t$$

$$PeriyodikVaryans = \sigma^2_{periodic} = \frac{1}{M}\sum_{t=1}^{M}(r_t - \mu_{periodic}$$

Yıllık Ortalama= $n\mu_{periyodik}$

Yıllık Varyans= $n\sigma^2_{periyodik}$

Yıllık Standart Sapma= $\sigma\sqrt{n}$

Bir hisse senedinin t zamanındaki fiyatı S_t ile gösterilsin. Lognormal dağılım, t ile $t + \Delta t$ tarihleri arasında (bir hisse senedini elde tutmanın getirisi + 1) doğal logaritmasının, μ ortalama ve σ standart sapma ile normal dağıldığını varsayar. Δt zaman dilimindeki bu getiri $r_{\Delta t}$ ile gösterilir. Bu durumda aşağıdaki eşitlik yazılabilir.

$$S_{t+\Delta t} = S_t e^{[r_{\Delta t}\Delta t]}$$

Lognormal dağılımda, Δt gibi kısa bir zaman dilimindeki $r_{\Delta t}$ getiri oranının, $\mu\Delta t$ ortalama ve $\sigma^2\Delta t$ varyans ile normal dağıldığı

varsayılır. Bu ilişkiyi yazmanın bir başka yolu da $t+\Delta t$ zamanında $S_{t+\Delta t}$ hisse senedi fiyatını aşağıdaki şekilde ifade etmektir.

$$\frac{S_{t+\Delta t}}{S_t} = e^{[\mu \Delta t + \sigma Z \sqrt{\Delta t}]}$$

formülde Z, standart normal dağılıma (0 ortalamaya ve 1 standart sapmaya) sahip bir degişkendir. Lognormal fiyat süreci geometrik dağılım gösterir.

$$\frac{dS}{S} = \mu dt + \sigma dB$$

formülde dB bir Wiener Sürecidir. Weiner Süreci ise $dB = Z\sqrt{dt}$ şeklinde ifade edilir.

Yukarıdaki varsayımın ne anlama geldiğini daha iyi anlamak için öncelikle standart sapmanın sıfır olduğu düşünülerek,

$$S_{t+\Delta t} = S_t e^{\mu \Delta t}$$

eşitliği elde edilir. Bu durumda hisse senedi fiyatının belirli bir oranda üstel olarak büyüdüğü söylenebilir. Bu haliyle hisse senedi, μ faiz oranı üzerinden Tablo 1'de örneklendiği gibi sürekli bileşik getiriye sahip risksiz tahvile benzer. (Çoşkun Y., 2018)

Tablo 1

	A	B	C	D	E	F
1				Rastsal sayı	Hisse fiyatı	
2	Getiri	15%	Dönem		35	
3	St. Sapma	30%	0	0,4002322	35,28796	
4	Zaman Dilimi	0,004	1	-2,0913103	33,93552	
5	Başlangıç Fiyatı	35	2	0,1115745	34,02784	
6			3	-0,813011	33,52707	
7			4	0,6258881	33,94796	
8			5	-0,3239256	33,7602	
9			6	2,8905924	35,6849	
10			7	-0,2000309	35,57106	
11			8	2,5671398	37,36896	
12			9	-1,767462	36,15825	
13			10	-0,7335711	35,67987	
14						

Hisse Senedi Fiyatlarının Lognormal Dağılım Parametrelerinin Hesaplanması

Bu noktada amacımız lognormal dağılımlarda ihtiyaç duyulan μ ve σ parametrelerini hesaplamak için hisse senedi fiyat verilerinin nasıl kullanılacağını göstermektir. Belirli bir Δt zaman aralığında hisse senedi getirisinin logaritmasının ortalama ve varyansına ilişkin formül aşağıda verilmiştir.

$$E[ln(\frac{S_{t+\Delta t}}{S_t})] = E[\mu\Delta t + \sigma Z\sqrt{\Delta t}] = \mu\Delta t$$

$$Var[ln(\frac{S_{t+\Delta t}}{S_t})] = Var[\mu\Delta t + \sigma Z\sqrt{\Delta t}] = \sigma^2\Delta t$$

Yukarıdaki ifadeler hem beklenen logaritmik getirinin hem de logaritmik getirilerinin varyansının zaman içinde doğrusal olduğu anlamına gelmektedir. Bu aşamada geçmişteki fiyat verilerinden lognormal μ ve σ tahmin etmek istendiğinde aşağıdaki formüllerin kullanılması gerekecektir.

$$\mu = \frac{ortalama[ln(S_{t+\Delta t}/S_t)]}{\Delta t}$$

$$\sigma^2 = \frac{Var[ln(S_{t+\Delta t}/S_t)]}{\Delta t}$$

Tablo 2

	A	B	C	D
1				
2	TARİH	FİYAT	GETİRİ	
3	Ağu.05	30,74		
4	Eyl.05	33,97	9,99%	
5	Eki.05	29,3	-14,79%	
6	Kas.05	31,62	7,62%	
7	Ara.05	30,78	-2,69%	
8	Oca.06	39,55	25,07%	
9	Şub.06	33,86	-15,53%	
10	Mar.06	36,35	7,10%	
11	Nis.06	38,91	6,81%	
12	May.06	37,21	-4,47%	
13	Haz.06	37,02	-0,51%	
14	Tem.06	33,29	-10,62%	
15	Ağu.06	32,62	-2,03%	
16	Eyl.06	28,45	-13,68%	
17	Eki.06	28,78	1,15%	
18				
19	Aylık ortalama	-0,47%		
20	Aylık st. Sapma	10,93%		
21				
22	Yıllık ortalama	-5,65%		
23	Yıllık st. Sapma	37,87%		
24				

Tablo 2 ’de yıllık ortalama logaritmik getiri, aylık ortalama logaritmik getirinin 12 ile çarpılması ile bulunurken, yıllık standartsapma, aylık standart sapma ile 12’nin karekökü çarpılarak bulunmaktadır. Genel bir ifade ile göstermek istenirse aşağıdaki eşitliğe ulaşılır.

$$\mu_{yıllık} = n.\mu_{periyodik}$$

$$\sigma_{yıllık} = \sqrt{n}\rho_{periyodik}$$

Rassal Yürüyüş Hipotezi ve Etkin Piyasalar Hipotezi

Yatırımcıların, hisse senedi piyasasında alım-satım kararı vermelerinde etkili olan tüm etkenler, sahip oldukları bilgilerin bir bileşkesi olarak düşünülmektedir. Etkin piyasa hipotezi, tüm yatırımcıların eş zamanlı olarak tüm bilgilere maliyetsiz ulaşabildiğini ve hisse senedi fiyatının bu bilgilerin yorumlanması ile ortaya çıkan alım satım kararları sonucu oluştuğu varsayımından hareket etmektedir. Bu durumda hisse senedinin fiyatı, tüm bilgileri yansıttığı için gerçek değerini göstermektedir ve yanlış fiyatlama olasılığı yoktur. Fiyat değişimleri, yeni bilgilerin piyasaya gelmesi ile yaşanmaktadır. Yeni bilgilerin ne olacağı ve etkisinin ne yönde olacağı bilinmeyeceği için hisse senedi fiyatlarının tamamıyla rassal olarak hareket edeceği varsayılır.

Etkin piyasalar hipotezinin varsayımları şu şekilde sıralanabilir:

- Birinci ve en önemli varsayım, piyasada birbirinden bağımsız çok sayıda yatırımcının var olduğudur. Yatırımcılar hisse senetlerinin değerlemesi ve analizi ile yakından ilgilenen kar maksimizasyonunu hedeflemiş kişilerdir. Hisse senedinin alım – satımı ile ilgili işlem maliyeti yoktur.

- Hisse senetlerine ilişkin haberler birbirinden bağımsız olarak rassal aralıklarla piyasaya ulaşmaktadır.
- Yatırımcılar, piyasaya ulaşan bir haberin etkisini hızlı bir şekilde piyasaya yansıtmaktadırlar. Ancak bu yansıma her zaman mükemmel bir şekilde olmadığı için fiyat oluşumuna ilişkin bir önyargı olusturmak mümkün değildir.

Yatırımcıların sayısının çok olması nedeniyle piyasaya ulaşan bir haberin fiyata yansıması hızlı olmaktadır. Piyasaya ulaşan haberlerin birbirinden bağımsız ve rassal olması ile birleştirildiğinde hisse senedi fiyat değişimine ilişkin olarak çıkan sonuç tamamıyla "bağımsız ve rassal" olduğudur. Piyasadaki yatırımcı sayısının fazlalığının yanında işlem hacminin miktarı da hipotezin geçerliliğini etkilemektedir. İslem miktarı ne kadar çok olursa hisse senedi fiyat değişimi o kadar hızlı yaşanmaktadır. (Çoşkun Y., 2018, Kaya S., 2020)

Hisse senedi fiyatları, piyasaya ulaşan bilgilerin tarafsız bir sonucu olması ve bu haberlerin rassal olması nedeniyle risk içermektedir ve hisse senedinin cari fiyatının bir parçası olan beklenen getiri bu riski yansıtmaktadır.

Etkin piyasa hipotezini tek bir Pazar biçimini anlatan model olarak düşünmek, hipotezin getireceği faydayı azaltacaktır. Piyasaya ulaşan haberlerin hisse senedi fiyatını yansıtma derecesine göre hipotez üç farklı şekilde ele alınmaktadır. (Çoşkun M., 2016)

- Zayıf Formda Etkin Piyasa Hipotezi: Hisse senedi cari fiyatlarının, hisse senedi piyasasına ilişkin bilgileri tam olarak yansıttığı piyasa türüdür. Hisse senedi geçmiş fiyat verileri, işlem hacmi ve diğer piyasa verileri bu bilgi setinin içindedir. Hisse senedinin geçmişteki fiyat verileri ile beklenen fiyat değişimleri arasında hiçbir ilişkinin olmadığı

varsayılır. Bu nedenle geçmişteki fiyat değişmeleri ve verilerinden hareketle oluşturulacak bir kurala dayalı fiyat tahminlerinin çok az bir değere sahip olacağı varsayılmaktadır.

- Yarı Etkin Formda Etkin Piyasa Hipotezi: Hisse senedi fiyatları kamuya açıklanan tüm bilgileri yansıtmaktadır. Kamuya açıklanan yeni bilgi, hisse senedi fiyatlarında düzeltmeye neden olmaktadır. Söz konusu veriler, kar payı, ekonomik haberler, politik haberler gibi piyasa ile ilgili olmayan bilgileri de kapsamaktadır. Yatırımcılar bu bilgilere kamuya açıklandığı anda sahip olmakta ve bir maliyete katlanmamaktadır. Bu nedenle elde edilen bilgilerin ortalama getiriden fazla kar sağlama özelliği yoktur.
- Güçlü Etkin Formda Piyasa Hipotezi: Hisse senedi fiyatlarının, kamuya açıklanan ve bunların yanında firma içi bilgiler adı verilen özel bilgileri de yansıtan piyasa türüdür. Kamuya açıklanmayan ve bazı yatırımcıların daha erken ulaşabildiği özel bilgilerin fiyatlara yansımış olması, bu bilgiler nedeniyle herhangi bir grubun ek kazanç sağlama olasılığı bulunmamaktadır.

Etkin piyasa hipotezinin geçerliliğini test etmek için hisse senedinin getirilerini açıklayan modellere ihtiyaç vardır. Oluşturulan modellerde hisse senedinin fiyat hareketi rassal yürüyüş teorisi ile açıklanmaktadır. (Çoşkun Y., 2018)

Monte Carlo Yöntemine Göre Modelleme

Monte Carlo (MC) Simülasyonu, bilinen parametreleri kullanan rassal simülasyon türlerinden biridir. Analitik çözüme ulaşılamadığı durumlarda modelin sayısal değerlerine ulaşmak için sıkça kullanılan MC modelinin temeli fiziğe dayanmaktadır. Finanstaki kullanımı da buna benzerdir. Analitik olarak kolay elde edilemeyen varlık fiyatlarının simülasyonu için kullanılmaktadır. Opsiyon sözleşmeleri (Avrupa Tipi opsiyonlar hariç) bu kategoriye en uygun finansal varlıklardır.

Monte Carlo Problemleri: Yatırım ve Emeklilik

Farklı yatırım seçeneklerinin değerlendirilmesi ve emeklilik planları arasında seçim yapmak Monte Carlo Simülasyonunun kullanıldığı alandır. Emeklilik ile ilgili olarak 1.000.000 TL'ye sahip olunduğunu ve yatırım araçlarından oluşan bir karışımın elde edilmeye çalışıldığı düşünülsün. %6 yıllık getirili risksiz bir tahvilin ve %12 yıllık bileşik getiri ve %30 getirinin standart sapması olan riskli bir hisse senedi portföyü olduğu varsayılsın. Her yıl hesaptan 150.000 TL almak ve 10 yıl sonra yatırımı nakde çevirmek istendiği farz edilsin.

Tablo 3

	A	B	C	D	E	F	G	H	I	J
1										
2	yatırım tutarı	1000000								
3	risksiz yatırımın getirisi	6%								
4	riskli yatırımın parametreleri									
5	yıllık beklenen getiri	8%								
6	getirinin standart sapması	20%								
7	riskli varlığın oranı	70%								
8	yıllık nakit çekimi	150000,00								
9										
10	YIL	yıl başı toplam değer	riskli yatırım tutarı	risksiz tatırım tutarı	normal dağılımlı rastsal sayı	1+ riskli yatırım getirisi	yıl sonu toplam değer	yıllık nakit çekimi	10 yıl sonu kalan değer	
11	1	1000000	700000	300000	0,1309	1,112022	1096966,4	150000		
12	2	946966,3797	662876,47	284089,9139	-0,1434	1,05266	999440,39	150000		
13	3	849440,3884	594608,27	254832,1165	1,3847	1,42895	1120255,6	150000		
14	4	970255,6221	679178,94	291076,6866	1,3607	1,422108	1274941,4	150000		
15	5	1124941,393	787458,98	337482,4179	0,6773	1,240432	1335140,8	150000		
16	6	1185140,764	829598,53	355542,2291	-1,2954	0,836039	1071104,5	150000		
17	7	921104,4731	644773,13	276331,3419	-1,3894	0,820468	822434,63	150000		
18	8	672434,6349	470704,24	201730,3905	-0,7985	0,923393	648849,86	150000		
19	9	498849,8575	349194,9	149654,9572	-1,5314	0,797495	437390,21	150000		
20	10	287390,2103	201173,15	86217,06308	-0,6802	0,945501	281757,9	150000	131757,9	
21										

Tablo 3'teki B kolonu her yılbaşındaki toplam serveti göstermektedir. Bu servet B7 hücresine bağlı olarak riskli ve risksiz varlığa bölünmektedir. Risksiz yatırım %6 sürekli bileşik (yatırım $e^{\%6}$) getiri sağlamaktadır. Yatırım riskli bölümü $e^{\mu+\sigma Z}$ faktörü ölçüsünde büyümektedir. Formülde Z, ortalaması 0 ve standart sapması 1 olan normal dağılıma sahip rassal bir sayıdır.

Riskli Varlığın Ağırlığını Belirleme Kuralı

Tablo 3'teki simülasyonda riskli ve risksiz varlıkların ağırlıkları mekanik olarak belirlenmişti. Çekilen paranın tutarı da hesapta kalan para ne olursa olsun aynı miktardaydı.

Aşağıda Tablo 4'te bu mekanik yaklaşım düzeltilmiş ve yatırımcının bir emniyet kuralı tanımladığı varsayılmıştır. Bu kurala göre her yıl sonunda kalan değerin, yıllık çekilen değerin en az 3 katı olması durumunda yıllık çekim miktarı 150.000 TL olacak ve aksi durumda yatırımcı portföyün değerinin üçte birini çekebilecektir.

Tablo 4

	A	B	C	D	E	F	G	H	I	J
1										
2	yatırım tutarı	1000000								
3	risksiz yatırımın getirisi	6%								
4	riskli yatırımın parametreleri									
5	yıllık beklenen getiri	8%								
6	getirinin standart sapması	20%								
7	riskli varlığın oranı	70%								
8	emniyet kuralı	3,00								
9	yıllık nakit çekimi	150000,00								
10										
11	YIL	yıl başı toplam değer	riskli yatırım tutarı	risksiz yatırım tutarı	normal dağılımlı rastsal sayı	1+ riskli yatırım getirisi	yıl sonu toplam değer	yıllık nakit çekimi	10 yıl sonu kalan değer	
12	1	1000000	700000	300000	-0,6804	0,945463496	980375,41	150000		
13	2	830375,411	581262,79	249112,62	-0,7282	0,936467932	808850,85	150000		
14	3	658850,848	461195,59	197655,25	-1,4288	0,81402842	585303,89	150000		
15	4	435303,893	304712,73	130591,17	1,2797	1,399255067	565037,3	150000		
16	5	415037,3	290526,11	124511,19	-0,699	0,941952905	405872,45	135291		
17	6	270581,445	189407,01	81174,434	-0,9397	0,897681456	256221,14	85407		
18	7	170814,142	119569,9	51244,243	0,7463	1,25766899	204792,36	68264		
19	8	136528,364	95569,855	40958,509	0,5553	1,210532082	159181,62	53061		
20	9	106120,618	74284,432	31836,185	1,0214	1,328804944	132514,35	44172		
21	10	88342,346	61839,642	26502,704	0,3635	1,164975434	100183,2	33395	66788,2035	
22										

Buna benzer birçok kural koyulabilir. Buradaki problem, bir yöneticinin eş zamanlı olarak yatırım ve çekme politikalarını nasıl belirleyeceğidir.

Finansal Yatırımlarda Model Oluşturma

Finansal model bir finansal varlığın fiyatı veya getirisinin matematiksel bir şekilde ifade edilmesidir. Finansal modellemede bir şirketin ihtiyacına ve yapısına göre şekillenen varsayımlar bulunmaktadır. Bu varsayımlar, şirketi etkileyecek bütün giderleri içerir. Bunlar enflasyon, faiz, kapasite kullanım oranı, yatırımın ekonomik süresi gibi.

Portföy Modeli Oluşturma

Portföy teorisi, Hary Markowitz, John Lintner, Jan Mossin, ve William Sharpe tarafından geliştirilmiştir. Portföy teorisinin nasıl işlediğini anlayabilmek için en basit haliyle iki varlıktan oluşan portföylere ilişkin hesaplamaların yapılması faydalı olacaktır.

Tablo 5

	A	B	C	D	E	F	G
1		FİYATLAR			GETİRİLER		
2	TARİH	A	B		A	B	
3	Tem.01	0,28	2,14				
4	Ağu.01	0,34	1,8		19,42%	-17,30%	
5	Eyl.01	0,32	1,28		-6,06%	-34,09%	
6	Eki.01	0,39	1,69		19,78%	27,79%	
7	Kas.01	0,4	3,44		2,53%	71,07%	
8	Ara.01	0,44	3,95		9,53%	13,82%	
9	Oca.02	0,5	3,49		12,78%	-12,38%	
10	Şub.02	0,4	2,79		-22,31%	-22,39%	
11	Mar.02	0,36	2,65		-10,54%	-5,15%	
12	Nis.02	0,41	2,6		13,01%	-1,90%	
13	May.02	0,36	2,6		-13,01%	0,00%	
14							

Tablo 5'te A ve B hisse senetlerinin tarihi fiyatlarından yararlanarak getirilerin hesaplanması verilmiştir. Hisse senetlerinin getirileri, yatırımcının her iki hisse senedini 2001 yılının haziran ayı sonunda (t-1 zamanı) satın aldığı ve 2002 yılı mayıs ayı sonuna kadar sürekli olarak izleyen ayın sonunda sattığı varsayımı ile hesaplanmıştır.

Bu durumda getirilere ilişkin temel formül $r_{it} = ln(\frac{P_{it}}{P_{it-1}})$ şeklindedir. Bu formülde getiriler, sürekli bileşik getiri esasına göre hesaplanmıştır. Bu hesaplamaya alternatif olarak kesikli getiriler kullanılmak istenirse $r_{it} = \frac{P_{it}}{P_{it-1}} - 1$ formülü kullanılmalıdır. İki yöntem de kullanılabilir. Ancak geçmişteki getirilere ait dağılımın gelecekte de aynı şekilde devam edeceği varsayımı ile geleceğe ilişkin ortalama periyodik getirinin elde edilebilmesi için sürekli bileşik getirinin kullanılması gerekmektedir. Geçmişteki fiyat hareketlerinin gelecek ile ilgili bazı bilgiler verdiği düşünülerek, verilerden elde edilen ortalama getiri beklenen aylık getiri olarak kullanılabilir.

Hisse senetlerinin beklenen getirilerini ve risk ölçülerini (varyans ve standart sapma) hesaplamak için Excelde ortalama, vars ve stdsapmas fonksiyonlarından yararlanılır. Varyans ve standart sapma için var ve stdsapma fonksiyonları yerine yukarıda belirtilen fonksiyonların kullanılmasının iki sebebi vardır. Bunlardan ilki tarihi verilerin gelecekteki değerlerin dağılımını gösterdiği varsayımıdır. Bu varsayım örneklem varyansı yerine ana kütle varyansının kullanılmasını gerektirmektedir. İkinci sebep ise Beta katsayısının hesaplanması ile ilgilidir.

İki hisse senedinin getirileri arasındaki ilişkiyi ölçmek amacıyla hesaplanan kovaryans;

$$Cov(r_A, r_B) = \frac{1}{M} \sum_t [r_{A,t} - E(r_{A,t})] * [r_{B,t} - E(r_{B,t}$$)]

formülü ile hesaplanmaktadır.

Tablo 6

	A	B	C	D	E	F	G	H	I	J
1		A				B				
2	TARİH	FİYAT	GETİRİ	r_A,t - E(r_A,t)		FİYAT	GETİRİ	r_B,t - E(r_B,t)		r_A,t - E(r_A,t) * r_B,t -E(r_B,t)
3	Tem.01	0,28				2,14				
4	Ağu.01	0,34	19,42%	15,95%		1,8	-17,30%	-17,43%		-0,0278
5	Eyl.01	0,32	-6,06%	-9,53%		1,28	-34,09%	-34,22%		0,0326
6	Eki.01	0,39	19,78%	16,32%		1,69	27,79%	27,66%		0,0451
7	Kas.01	0,4	2,53%	-0,93%		3,44	71,07%	70,95%		0,0066
8	Ara.01	0,44	9,53%	6,07%		3,95	13,82%	13,70%		0,0083
9	Oca.02	0,5	12,78%	9,32%		3,49	-12,38%	-12,51%		-0,0117
10	Şub.02	0,4	-22,31%	-25,78%		2,79	-22,39%	-22,51%		0,058
11	Mar.02	0,36	-10,54%	-14,00%		2,65	-5,15%	-5,28%		0,0074
12										
13		A	B							
14	aylık ort.	3,14%	2,67%							
15	aylık var.	0,019949	0,101259							
16	aylık s.p.	14,12%	31,82%							
17										
18	kovaryans 1	0,014813								
19	kovaryans 2	0,013261								
20										
21	korelasyon 1	0,033372								
22	korelasyon 2	0,294938								
23										

Tablo 6'da kovaryansa nazaran yorumlanması daha kolay olan korelasyon katsayısının hesaplanması ile hisse senetleri arasındaki ilişki daha açık olarak görülmektedir. Kullanılan değerlere ait birimlerden bağımsız olarak getiriler arasındaki doğrusal ilişkinin derecesini ve yönünü gösteren korelasyon

katsayısı +1 ve -1 arasındaki değerleri alabilmektedir. +1 pozitif tam olumlu ve -1 negatif tam olumsuz korelasyonu temsil etmektedir. Getiriler arasında ilişki olmaması durumunda ise sıfır değerini almaktadır.

İki hisse senedinden oluşturulacak bir portföye ilişkin risk ve getirinin hesaplanması, her bir varlığa ilişkin hesaplamalara benzer şekilde ortalama ve varyansların hesaplanması gerektirmektedir. Portföyün ortalama beklenen getirisi, iki varlığın beklenen getirilerinin portföydeki payları ile ağırlıklı ortalamasıdır.

$$E(r_p) = w_A * E(r_A) + w_B * E(r_B)$$

Ancak portföyün varyansı için aynı mantıkla hesaplama yapmak mümkün değildir. İki varlığın bir arada bulunmasının risk üzerindeki etkisini yansıtacak bir terimin hesaba katılması gerekmektedir.

$$Var(r_p) = w_A^2 * Var(r_A) + w_B^2 * Var(r_B) + 2 * w_A w_B Cov(r_A, r_B)$$

Aynı formül degişkenler arasındaki kovaryansı kullanmak yerine korelasyon katsayısı kullanılarak yazılmak istenirse aşağıdaki gibi olur.

$$\sigma_P^2 = \omega_A^2 * \sigma_A^2 + \omega_B^2 * \sigma_B^2 + 2 * \omega_A * \omega_B * \rho_{A,B} * \sigma_{A,B}$$

Tablo 7

	A	B	C	D
1		A	B	
2	ORTALAMA	3,47%	0,13%	
3	VARYANS	0,018	0,03	
4	STANDART SAPMA	13,34%	17,43%	
5	KOVARYANS	0,0092		
6	PORTFÖY AĞIRLIKLARI	0,5		
7	PORTFÖYÜN GETİRİSİ	0,018		
8	PORTFÖYÜN VARYANSI	0,0166		
9	PORTFÖYÜN ST. SAPMASI	0,128841		
10				

İki varlıktan oluşan bir portföyün risk ve getirisini hesaplamak portföy mantığının anlaşılması açısından oldukça faydalıdır. Ancak ikiden fazla varlıktan oluşan portföyler için hesaplamaların yapılması genel bir form elde edilmesini sağlayacaktır. Bu form varyans- kovaryans matrisinin elde edilmesini gerektirmektedir.

N varlıktan oluşan bir portföy için, her varlığın portföydeki ağırlığının x_i ve beklenen getirilerin E(r) ile gösterilmesi durumunda vektörel gösterim

$$\mathrm{x} = \begin{bmatrix} \mathrm{x}_1 \\ \mathrm{x}_2 \\ \vdots \\ \mathrm{x}_\mathrm{N} \end{bmatrix}$$

$$E(r) = \begin{bmatrix} E_{r_1} \\ E_{r_2} \\ \vdots \\ E_{r_N} \end{bmatrix}$$

biçimindedir. Sütun vektörü olarak gösterilen x portföy bileşimi ve getirisinin transpozesi alınarak satır vektörleri elde edilir.

$$x^T = [x_1, x_2, \ldots, x_N]$$

$$E(r)^T = [E(r_1), E(r_2), \ldots, E(r_N)]$$

Satır vektörleri elde edilir. Portföyde yer alan her bir varlığın getirisini portföydeki payı ile ağırlıklandırıldığında portföyün beklenen getirisi

$$E(r_x) = \sum_{i=1}^{n} x_i E(r_i)$$

olur. Matris notasyonu ile gösterimi ise

$$E(r_p) = \sum_{i=1}^{n} x_i E(r_i) = x^T E(r) = E(r)^T x$$

biçimindedir. Portföyün riskini gösteren genel varyans formülü

$$Var(r_x) = \sum_{i=1}^{N} (x_i)^2 Var(r_i) + 2 \sum_{i}^{N} \sum_{j=i+1}^{N} x_i x_j Cov(r_i, r_j)$$

formüldeki ilk terim, portföyde bulunan her bir varlığın ağırlıklarının karesi ile varyansının çarpımını ifade etmektedir. İkinci terim ise her bir varlık çiftinin birbirleriyle olan kovaryansının varlıklarının ağırlıkları ile çarpımının iki katını göstermektedir.

İkiden fazla varlıktan oluşan portföylerin varyansını matris notasyonu ile göstermek oldukça kolaylaştırıcı işleve sahiptir. Elde edilen varyans – kovaryans matrisinde yer alan terimlere ait genel ifade σ_{ij} ,seklindedir. Matriste i satır j sütun indisi olarak kullanılmaktadır.

$$S = \begin{bmatrix} \sigma_{11} & \sigma_{12} & \cdots & \sigma_{1N} \\ \sigma_{21} & \sigma_{22} & \cdots & \sigma_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{N1} & \sigma_{N2} & \cdots & \sigma_{NN} \end{bmatrix}$$

Portföy varyansının matris gösterimi ise $Var(r_p) = x^T S x$,seklinde olacaktır.

Tablo 8

	A	B	C	D	E	F	G
1		Varyans - Kovaryans Matrisi					
2		A	B	C	D	ORT. GETİRİ	
3	A	0,1	0,01	0,03	0,05	6%	
4	B	0,01	0,3	0,06	-0,04	8%	
5	C	0,03	0,06	0,4	0,02	10%	
6	D	0,05	-0,04	0,02	0,5	15%	
7							
8	Port. Ağır.	A	B	C	D		
9	Portföy X	0,2	0,3	0,4	0,1		
10							
11		X Portföyü					
12	Getiri	9,10%					
13	Varyans	12,16%					
14							

Tablo 8'de oluşturulan X portföyünde bulunan varlıkların varyans – kovaryans matrisi incelendiğinde, varlıkların A'dan D'ye doğru risklerinin yükseldiği görülmektedir. Oluşturulan X portföyünde varlıkların ağırlıklarına bakıldığında ılımlı bir risk tercih edildiği görülmektedir. Yatırımcının farklı risk tercihlerinin portföyün getiri ve risk ölçülerine olan etkisini görebilmek için riski daha yüksek Y portföyü aşağıda Tablo 9'da oluşturulmuştur.

Tablo 9

	A	B	C	D	E	F	G	H	I	J
1										
2		A	B	C	D	Ort. Getiri			X Port.	Y Port.
3	A	0,1	0	0,03	0,05	6%		Getiri	9,10%	12,00%
4	B	0,01	0,3	0,06	-0,04	8%		varyans	0,121	0,2032
5	C	0,03	0,06	0,4	0,02	10%		kovaryans(x,y)	0,0712	
6	D	0,05	-0,04	0,02	0,5	15%		korelasyon(x,y)	0,454073	
7								X Port. Ağır.	0,3	
8	Port. Ağır.	A	B	C	D			Port(x,y) getiri	11,13%	
9	Portföy X	0,2	0,3	0,4	0,1			port(x,y) varyans	14,04%	
10	Portföy Y	0,2	0,1	0,1	0,6			port(x,y) St. Sapma	37,46%	
11										

Piyasa Portföyü

Piyasa portföyü M, piyasadaki tüm riskli varlıkların bileşiminden oluşan bir portföydür. Piyasada N sayıda riskli varlık olduğunu ve i varlığının piyasa değerinin V_i olduğunu varsayalım. Bu durum da piyasa portföyü aşağıdaki ağırlıklara sahip olacaktır.

M portföyünde i varlığın oranı;

$$\frac{V_i}{\sum_{h=1}^{N} V_h}$$

M piyasa portföyü etkin ise, piyasa portföyü için SML geçerlidir;

$$E(r_x) = E(r_z) + \beta_x[E(r_M) - E(r_z)]$$

$$\beta_x = \frac{Cov(x, M)}{\sigma_M^2}$$

$$Cov(z, M) = 0$$

Eğer tüm yatırımcılar portföylerini sadece portföyün ortalaması ve varyansına göre seçerlerse bu varsayımda söz edilen x portföyü M piyasa portföyüdür. (Kaya S., 2020)

Piyasa Doğrusu: Piyasa Portföyünün Bulunması

Risksiz bir varlığın var olduğu ve getirisinin r_f ile ifade edildiği varsayılsın. Aşağıdaki eşitliklerin çözümünden M etkin portföyünün elde edildiği farz edilsin.

$$E(r) - r_f = S_z$$

$$M_i = \frac{z_i}{\sum_{i=1}^{N} z_i}$$

Önce M portföyü ve risksiz varlığın konveks bir kombinasyonu oluşturulur. Örneğin oluşturulacak portföyde risksiz varlığın ağırlığı a ile gösterilsin. Oluşturulan portföyün getirisi standart sapması ile ilgili

$$E(r_p) = ar_f + (1 - a)E(r_M)$$

$$\sigma_p = \sqrt{a^2\sigma_{r_f} + (1-a)^2\sigma_M^2 + 2a(1-a)Cov(r_f, r_y)} = (1-a)\sigma_M$$

Eşitlikleri oluşturabilir. a ≥ 0 için kombinasyonların bulunduğu alan Piyasa Doğrusu (CML) olarak bilinir. (Çoşkun M.,2016, Kaya S.,2020)

Varyans- Kovaryans Matrisinin Hesaplanması

M dönem için N adet varlığın getiri verilerine sahip olunduğunu varsayalım. Herhangi bir t tarihinde i varlığın getirisi r_{it} ile gösterilir ve i varlığın ortalama getirisi

$$r_i = \frac{1}{M}\sum_{t=1}^{M} r_{it}$$

ile hesaplanır. i ve j varlıklarının getirileri arasındaki kovaryansın formülü ise

$$\sigma_{ij} = Cov(i,j) = \frac{1}{M-1}\sum_{t=1}^{M}(r_{it} - r_i) * (r_{jt} - r_i$$

biçimindedir. Yukarıdaki formül ile elde edilen kovaryansların matrisi (i= j) basit varyans- kovaryans matrisidir. Ancak asıl sorun bu kovaryansların hesaplanmasıdır. Bunun için öncelikle *A* artık getiri matrisi tanımlanır.

$$A = \begin{bmatrix} r_{11} - r_1 & \cdots & r_{N1} - r_N \\ \vdots & \ddots & \vdots \\ r_{1M} - r_1 & \cdots & r_{NM} - r_N \end{bmatrix}$$

A matrisinin sütunlarını, her bir varlığın getirilerinden ortalama varlık getirisini çıkararak elde ederiz. Bu matrisin transpozesi alınarak

$$A^T = \begin{bmatrix} r_{11} - r_1 & r_{12} - r_1 & \cdots & r_{1M} - r_1 \\ \vdots & \vdots & \ddots & \vdots \\ r_{N1} - r_1 & r_{N2} - r_1 & \cdots & r_{NM} - r_N \end{bmatrix}$$

matrisi bulunur. A^T ile A matrisleri çarpılıp M – 1'e bölünerek

$$S = [\sigma_{ij}] = \frac{A^T * A}{M - 1}$$

varyans – kovaryans matrisi elde edilir.

Aşağıda 6 hisse senedine ait getiri verilerinden yararlanılarak Tablo 10 oluşturulmuştur.

Tablo 10

	A	B	C	D	E	F	G	H
1								
2	FİYAT VERİLERİ							
3	Tarih	A	B	C	D	E	F	
4	Ara.08	3,58	53,6	619,75	0,5	0,56	0,18	
5	Oca.09	3,58	51,85	565,21	0,44	0,57	0,17	
6	Şub.09	3,35	54,92	659,42	0,48	0,61	0,14	
7	Mar.09	3,88	60,63	783,37	0,51	0,84	0,17	
8	Nis.09	4,38	71,5	738,75	0,7	1,02	0,19	
9	May.09	5,25	70,5	740	0,71	1,23	0,25	
10	Haz.09	5,65	76,5	785	0,77	1,25	0,23	
11	Tem.09	6,1	77,5	780	1,05	1,37	0,24	
12	Ağu.09	6,2	76	810	1,34	1,36	0,27	
13	Eyl.09	7	74,5	1525	2,16	1,24	0,28	
14	Eki.09	6,5	80,5	1510	1,43	1,09	0,79	
15	Kas.09	5,75	73	1505	1,46	1	1,56	
16								
17	His. Snd. Sayısı	10,56	10,86	2,97	0,41	0,84	0,79	
18	Piyasa değeri	60,72	792,78	4469,85	0,5986	0,84	1,2324	
19	Portföy Oranı	1,14%	14,89%	83,92%	0,01%	0,02%	0,02%	
20								
21	Getiri Verileri	A	B	C	D	E	F	
22	Oca.09	0,00%	-3,32%	-9,21%	-12,78%	1,77%	-5,72%	
23	Şub.09	-6,64%	5,75%	15,42%	8,70%	6,78%	-19,42%	
24	Mar.09	14,69%	9,89%	17,22%	6,06%	31,99%	19,42%	
25	Nis.09	12,12%	16,49%	-5,86%	31,67%	19,42%	11,12%	
26	May.09	18,12%	-1,41%	0,17%	1,42%	18,72%	27,44%	
27	Haz.09	7,34%	8,17%	5,90%	8,11%	1,61%	-8,34%	
28	Tem.09	7,66%	1,30%	-0,64%	31,02%	9,17%	4,26%	
29	Ağu.09	1,63%	-1,95%	3,77%	24,39%	-0,73%	11,78%	
30	Eyl.09	12,14%	-1,99%	63,27%	47,74%	-9,24%	3,64%	
31	Eki.09	-7,41%	7,75%	-0,99%	-41,24%	-12,89%	103,72%	
32	Kas.09	-12,26%	-9,78%	-0,33%	2,08%	-8,62%	68,04%	
33								
34	Ort. Getiri	4,31%	2,81%	8,07%	9,74%	5,27%	19,63%	
35	St. Sapma	9,99%	7,49%	19,98%	24,17%	13,81%	36,13%	
36	Varyans	0,00999	0,00561	0,03992	0,05844	0,01908	0,13052	
37								
38	Artık Getiriler	A	B	C	D	E	F	
39	Oca.09	-4,31%	-6,13%	-17,28%	-22,53%	-3,50%	-25,35%	
40	Şub.09	-10,95%	2,94%	7,35%	-1,04%	1,51%	-39,05%	
41	Mar.09	10,38%	7,08%	9,16%	-3,68%	26,72%	-0,22%	
42	Nis.09	7,81%	13,68%	-13,93%	21,93%	14,14%	-8,51%	
43	May.09	13,81%	-4,22%	-7,90%	-8,32%	13,45%	7,81%	
44	Haz.09	3,04%	5,36%	-2,16%	-1,63%	-3,66%	-27,97%	
45	Tem.09	3,36%	-1,51%	-8,70%	21,27%	3,90%	-15,38%	
46	Ağu.09	-2,68%	-4,76%	-4,29%	14,65%	-6,00%	-7,85%	
47	Eyl.09	7,83%	-4,80%	55,21%	38,00%	-14,51%	-15,99%	
48	Eki.09	-11,72%	4,94%	-9,05%	-50,99%	-18,16%	84,09%	
49	Kas.09	-16,57%	-12,59%	-8,40%	-7,67%	-13,89%	48,41%	
50								
51		A	B	C	D	E	F	
52	X	0,00999	0,00253	0,00524	0,01176	0,0092	-0,0145	
53	Y	0,00253	0,00561	-0,0015	-4E-05	0,0051	-0,0032	
54	Z	0,00524	-0,0015	0,03992	0,02488	-0,00507	-0,0162	
55	T	0,01176	-4E-05	0,02488	0,05844	0,00659	-0,053	
56	K	0,0092	0,0051	-0,0051	0,00659	0,01908	-0,0187	
57	N	-0,0145	-0,0032	-0,0162	-0,053	-0,0187	0,13052	
58								
59								

Global Minimum Varyanslı Portföyün Hesaplanması

Varyans – kovaryans matrisinin en çok kullanıldığı iki yer global minimum varyanslı portföyün (GMVP) ve etkin portföylerin bulunmasıdır. Bir S varyans – kovaryans matrisine sahip N adet varlığın elde olduğu varsayılsın. GMVP, olası tüm etkin portföyler arasında en düşük varyansa sahip olan $x = [x_1,..,x_N]$ portföyü olarak gösterildiğinde aşağıdaki şekilde tanımlanır.

$$x_{GMVP} = \left[x_{GMVP,1}, x_{GMVP,2}, \dots, x_{GMVP,N}\right] = \frac{1.S^{-1}}{1.S^{-1}.1^T}$$

Minimum varyanslı portföyün en belirgin özelliği, hesaplanması sırasında varlığın beklenen getirisine ihtiyaç duyulmayan etkin sınır üzerindeki tek portföydür. Minimum varyanslı portföyün getirisi ve varyansı aşağıdaki şekilde verilebilir.

$$\mu_{GMVP} = x_{GMVP}.E(r)$$

$$\sigma^2_{GMVP} = x_{GMVP}.S_{x_{GMVP}}$$

Yukarıdaki formülleri kullanarak Excel yardımıyla varyans – kovaryans matrisini kullanarak global minimum varyanslı portföy getiri ve riski aşağıda Tablo 11'de hesaplanmıştır.

Tablo 11

	A	B	C	D	E	F	G	H
51		A	B	C	D	E	F	
52	X	0,009987	0,002534	0,005243	0,011757	0,009196	-0,01452	
53	Y	0,002534	0,00561	-0,00147	-4,3E-05	0,005099	-0,00317	
54	Z	0,005243	-0,00147	0,039919	0,024876	-0,00507	-0,01617	
55	T	0,011757	-4,3E-05	0,024876	0,058441	0,006593	-0,05302	
56	K	0,009196	0,005099	-0,00507	0,006593	0,019076	-0,0187	
57	N	-0,01452	-0,00317	-0,01617	-0,05302	-0,018695	0,130519	
58								
59	ORTALAMA	4,31%	2,81%	8,07%	9,74%	5,27%	19,63%	
60								
61		A	B	C	D	E	F	
62		0,167264	0,540187	0,075335	0,07845	0,036138	0,102626	
63								
64	TOPLAM	1						
65								
66	GMVP Getiri	0,058146						
67	GMVP Varyans	0,003199						
68	GMVP St. Sapma	0,056558						
69								

Etkin Portföyün Hesaplanması

Etkin portföy oluşturmaya ilişkin aşağıdaki eşitliği çözmek ilk adım olacaktır.

$$\frac{S^{-1}[E(r)-c]}{\sum S^{-1}[E(r)-c]}$$

Formülde S: varyans kovaryans matrisini, *E*(*r*): beklenen getiri vektörünü ve c: sabit getiriyi göstermektedir. Söz konusu formülü kullanarak Tablo 12 Excel tabloları ile etkin portföy hesaplanabilir.

Tablo 12

	A	B	C	D	E	F	G	H	I
1									
2		A	B	C	D	E	F		Ortalama Getiri
3	X	0,009987	0,002534	0,005243	0,011757	0,009196	-0,01452		4,31%
4	Y	0,002534	0,00561	-0,00147	-0,000043	0,005099	-0,00317		2,81%
5	Z	0,005243	-0,00147	0,039919	0,024876	-0,00507	-0,01617		8,07%
6	T	0,011757	-0,000043	0,024876	0,058441	0,006593	-0,05302		9,74%
7	K	0,009196	0,005099	-0,00507	0,006593	0,019076	-0,0187		5,27%
8	N	-0,01452	-0,003172	-0,06171	-0,053022	-0,0187	0,130519		19,63%
9	risksiz getiri oranı	2%							
10									
11		A	B	C	D	E	F		
12	Etkin Portföy	-27,60%	-0,07%	12,69%	33,35%	48,93%	32,71%		
13									
14	Piyasa değeri	336,44	305,82	152,93	15,44	41,01	16,98		
15	piyasa oranları	38,73%	35,21%	17,61%	1,78%	4,72%	1,95%		
16									
17									

Opsiyon Fiyatlama Teorisi

Opsiyon fiyatlama teorisinde ilk bilimsel gelişme 1877 yılında Charles Castelli tarafından yazılan "The Theroy of Options in Stocks and Shares" isimli kitap ile olmuştur. Castelli kitabında opsiyonların hedging ve spekülasyon yönünü tanıtmakla birlikte teorik bir temel sunamamıştır. 23 yıl sonra Louis Bachelier, "Theorie de la Speculation" isimli matematik tezinde opsiyonlar için bilinen ilk analitik değerlemeyi ortaya koymuştur. Bachelier'in çalışmasıyla ilgilenen Saul Samuelson 1965 yılında "Hisse Senedi Piyasasındaki

Brownian Hareketi" isimli makalesi ile hisse senetlerinin fiyat hareketlerinin izleyeceği yolu açıklamaya çalışmıştır. Aynı yıl Samuelson'un öğrencisi olan Kruizenga, "Alım ve Satım Opsiyonları: Bir Teori ve Pazar Analizi" isimli teziyle Bachelier'in tezini tekrar gündeme getirmiştir. 1962 yılında ise A. James Boness, "A Theory and Measurment of Stock Option Value" isimli tezi ile opsiyon fiyatlama teorisinde önemli bir adım atmıştır. (Çoşkun M.,2016, Kaya S., 2020)

Opsiyon fiyatlama teorisinde söz edilen çalışmalardan sonra en önemli adım 1973 yılında Myron Scholes ve Fischer Black tarafından atılmıştır. İlk olarak Black, hisse senedi varantları için bir değerleme modeli yaratmış ve bir varantın zamana ve hisse senedinin fiyatına bağlı olarak iskonto oranının nasıl değiştiğini gösteren bir türev ifadesi bulmuştur. Bu gelişmeden sonra Black ve Scholes birlikte opsiyon fiyatlama formülünü yaratmışlardır. Black-Scholes modeli, kendisinden önceki modellerin geliştirilmiş bir sonucu olmuştur. Aynı tarihte Merton, Black-Scholes'un ulaştığı sonuca kendi çalışmaları sonucunda ulaşmıştır.

Black-Scholes, Boness'un ortaya koyduğu modelde risksiz faiz oranının doğru iskonto faktörü olduğunu ve yatırımcıların risk tercihlerinin etkili olmadığını ispatlamışlardır. Aynı yıl Standford üniversitesinde finans profesörü olan William Sharpe daha basit matematiksel temelli olan bir formül ile Black ve Scholes'un elde ettiği sonuçlara ulaşmıştır.

Black – Scholes opsiyon fiyatlama formülü, arbitrajın olmadığı bir ortamda riskten korunma kavramına dayandırılmıştır. Formülü ilk olarak Avrupa tipi alım opsiyonları için türetilmiş, daha sonra yapılan çalışmalar ile diğer opsiyon türleri için kullanılabilir hale getirilmeye çalışılmıştır. Ayrıca formülün gerçeğe uygun

olmayan varsayımlarını ortadan kaldırmak için de çalışmalar yapılmıştır. (Çoşkun M.,2016, Çoşkun Y.,2018)

Bu çalışmalardan ilki Scholes tarafından formülün vergiler konusunda düzeltilmesidir. Daha sonra hisse senedi opsiyonlarında sözleşmeye konu olan varlığın kar payı dağıtımına ilişkin Merton (1973), Roll (1977), Geske (1979), Rubinstein ve Cox (1981) tarafından düzeltmeler yapılmıştır. Merton 1973 yılındaki çalışmasında faiz oranındaki değişmelerin opsiyonun değerinde yaratacağı etkiye değinmiştir. (Kaya S., 2020)

Opsiyon fiyatlama teorisinde Black-Scholes' dan sonra ikinci önemli gelişme sözleşme konusu varlığın fiyatının ve buna bağlı olarak opsiyon değerinin stokastik süreç izleyeceği varsayımıdır. Bu konudaki ilk çalışmalar Cox ve Ross (1976) ile Merton (1976) tarafından yapılmıştır. (Kaya S., 2020)

1979 yılında Harrison ve Kreps çok zamanlı ortamlarda opsiyonun değerini incelemiş, 1981 yılında ise Harrison ve Pliska opsiyon fiyatlamada Martingale teorisinin kullanımı öngörmüştür. Bu düşünceyi Martingale teorisini daha detaylı inceleyerek 1993 yılında Shiriaev tamamlamış ve Amerikan, Asya ve Rusya tipi opsiyonlar için genişletmişlerdir. 1994 yılında Gerber ve Shui opsiyonlar için yeni bir araç olarak Esscher dönüşümünü kullanmıştır. Eberlein ise 1995 yılında Esscher dönüşümünü hiperbolik türdeki Levy dağılımlarına uygulamıştır. Bardorff ve Nielsen ise bu dönüşümü Normal-Inserve-Gaussian dağılımlı Levy süreçleri için kullanılmıştır. (Çoşkun Y.,2018, Kaya S., 2020)

1996 yılında Hurst, Platen ve Rachev stokastik süreçlerin ikinci derecede zamanlarına ilişkin Bocher teorisini uygulayarak sürekli olarak kullanılabilecek bir opsiyon fiyatlama formülü

oluşturmuştur. Son olarak Duan, GARCH – Opsiyon fiyatlama üzerine çalışmıştır. (Çoşkun Y.,2018, Kaya S., 2020)

Sonuç

Teknolojik gelişmeler paralelinde dünya genelindeki nüfus artış hızına da bağlı olarak finans alanında üretilen pek çok veri bilgiye dönüştürülememektedir. Finansal verilerin teknolojik donanım ve yazılımlar kullanılarak işlenebilir bilgiye dönüştürülmesi süreci, uygulamaya dönük bilgi düzeyinin artmasıyla mümkündür. Bu çalışmada da finansal modelleme türleri yardımıyla finansal verilerin bilgisayar ortamında entegrasyonunu sağlamak yolunda uygulamaya dönük örnekler ile açıklamaya çalışılmıştır.

Kaynakça

Aydın N., Başar M., Çoşkun M. (2025). *Finansal Yönetim.* Ankara: Detay Yayıncılık

Benninga S. (2014). *Financial Modeling*. Cambridge: Mit Press

Beyazıt M.F. (2023). *Finansal Modelleme, Analitik ve Nümerik Çözümler*. Ankara: Seçkin Yayıncılık

Coşkun M. (2016). *Sermaye Bütçelemesi Kararlarında Finansal Modelleme*. Ankara: Detay Yayıncılık

Coşkun Y. (2018). *Finansal Yatırımlarda Model Oluşturma.* Ankara: Akademisyen Kitabevi

Haksever Ö. (2024). *İşletmelerde Finansal Modelleme Uygulaması*. İstanbul: Hiper yayın

Karacabey A.A. (2008). *Finansal Modelleme.* Ankara: Siyasal Kitabevi

Kaya S. (2020). *Finansal Modelleme*. İstanbul: Cinius Yayınları

Sayıner M.A. (2024). *Finansal Yönetim, Excel Ortamında Hesaplamalar, Modellemeler ve Optimizasyon İşlemleri*. Ankara: Nobel Akademik Yayıncılık

BÖLÜM 4

YAPAY ZEKÂ DESTEKLİ SİBER TEHDİT İSTİHBARATI

Tevfik FİRUZAN GÜLÇELİK [1*]
Onur SEVLİ [2]

Giriş

Dijital dönüşüm, bulut bilişim, nesnelerin interneti, uzaktan çalışma modelleri, yapay zekâ tabanlı uygulamalar ve veri odaklı iş süreçleri kurumların siber tehdit yüzeyini önemli ölçüde genişletmiştir. Kurumlar artık yalnızca kendi veri merkezlerinde konumlanan sınırlı sistemleri değil; bulut servislerini, mobil cihazları, üçüncü taraf entegrasyonlarını, tedarik zinciri bağlantılarını, kimlik yönetimi altyapılarını ve sürekli veri üreten dağıtık dijital ekosistemleri korumak zorundadır. Bu dönüşüm, siber güvenliği yalnızca teknik bir bilgi işlem fonksiyonu olmaktan

[1] Burdur Mehmet Akif Ersoy Üniversitesi, Eğitim Bilimleri Enstitüsü, Bilgisayar ve Öğretim Teknolojileri Eğitimi, Orcid: 0009-0009-3065-1895
[2] Doç. Dr., Burdur Mehmet Akif Ersoy Üniversitesi, Bilgisayar Mühendisliği, Orcid: 0000-0002-8933-8395

çıkarmış; kurumsal süreklilik, veri mahremiyeti, finansal güvenlik, itibar yönetimi ve ulusal güvenlik açısından stratejik bir risk yönetimi alanına dönüştürmüştür. Bu değişim, siber güvenliğin kurumsal risk yönetimiyle bütünleşik ele alınması gerektiğini ortaya koymaktadır (Nist, 2024).

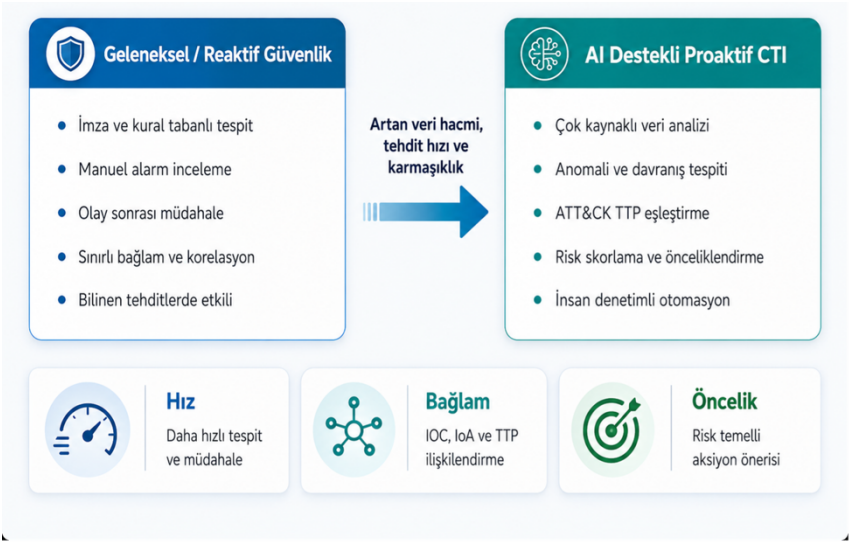
Siber tehdit ortamı yalnızca hacim olarak değil, nitelik olarak da değişmektedir. Geleneksel dönemde daha çok bilinen zararlı yazılım imzaları, basit ağ saldırıları ve sınırlı ölçekli güvenlik olayları öne çıkarken; günümüzde fidye yazılımı ekosistemleri, tedarik zinciri saldırıları, gelişmiş kalıcı tehditler, kimlik avı kampanyaları, bulut yanlış yapılandırmaları, sıfırıncı gün zafiyetleri ve yapay zekâ destekli sosyal mühendislik girişimleri daha karmaşık bir saldırı yüzeyi oluşturmaktadır. Saldırganlar otomasyon, açık kaynak araçlar, kiralanabilir saldırı altyapıları ve üretken yapay zekâ çözümleri sayesinde daha hızlı, daha ölçeklenebilir ve daha ikna edici saldırı senaryoları geliştirebilmektedir. Bu nedenle kurumların yalnızca bilinen tehditleri imza veya statik kurallarla tespit eden reaktif güvenlik yaklaşımlarına dayanması yeterli değildir.

Modern siber güvenlik yaklaşımı, olay meydana geldikten sonra tepki vermenin ötesine geçerek tehdidi önceden anlamayı, saldırgan davranışını modellemeyi, kurum varlıkları açısından gerçek riski değerlendirmeyi ve savunma önceliklerini istihbaratla belirlemeyi gerektirmektedir. Bu noktada siber tehdit istihbaratı, ham güvenlik verisini karar verilebilir bilgiye dönüştüren kritik bir güvenlik fonksiyonu olarak öne çıkmaktadır. Siber tehdit istihbaratı; tehdit aktörleri, saldırı teknikleri, taktikler, prosedürler, göstergeler, zafiyetler, hedeflenen sektörler ve olası etkiler hakkında bağlamsal bilgi üretmeyi amaçlar. Bu yönüyle siber tehdit istihbaratı (Cyber Threat Intelligence, CTI), yalnızca IP adresi, domain, hash veya

zararlı URL listelerinden ibaret değildir. Bir göstergenin hangi saldırı kampanyasıyla ilişkili olduğu, hangi tehdit aktörü tarafından kullanıldığı, hangi saldırı aşamasında görüldüğü, kurumun hangi varlıklarını etkileyebileceği ve hangi savunma aksiyonlarını gerektirdiği bilindiğinde gerçek anlamda istihbarat değeri ortaya çıkar. Bu bağlamda CTI, kurumların siber tehdit bilgisini toplama, değerlendirme ve paylaşma süreçlerini karar destek mekanizmasına dönüştüren bir yapı olarak değerlendirilmektedir (Nist, 2016; Brown ve Sfakianakis, 2025).

Bununla birlikte yapay zekâ destekli CTI, insan analistin yerine geçen bağımsız ve hatasız bir karar mekanizması olarak değerlendirilmemelidir. Yapay zekâ modelleri yanlış pozitif sonuçlar üretebilir, eksik veya hatalı veriyle beslendiğinde yanıltıcı istihbarat oluşturabilir, halüsinasyon nedeniyle gerçekte var olmayan göstergeler veya kaynaklar üretebilir, adversarial saldırılarla yanıltılabilir ya da hassas güvenlik verilerinin mahremiyetini riske atabilir. Bu nedenle yapay zekâ destekli CTI sistemleri açıklanabilirlik, denetlenebilirlik, veri kalitesi, model dayanıklılığı, insan onayı ve mevzuat uyumu ilkeleriyle birlikte tasarlanmalıdır. Özellikle kritik aksiyonlarda model çıktısının doğrudan otomatik müdahaleye dönüşmesi yerine, analiste gerekçeli öneri sunan insan denetimli bir karar destek yaklaşımı daha güvenli ve sürdürülebilir bir modeldir. Reaktif güvenlikten yapay zekâ destekli proaktif CTI'ye geçiş süreci Şekil 1'de özetlenmektedir. Bu nedenle yapay zekâ destekli CTI uygulamalarında güvenilirlik, açıklanabilirlik ve insan denetimi ilkeleri temel alınmalıdır (Nist, 2023; Balasubramanian vd., 2025; Mohamed, 2025).

Şekil 1. Reaktif Güvenlikten Yapay Zekâ Destekli Proaktif CTI'ye Geçiş



Siber Tehdit İstihbaratı Kavramı ve Yaşam Döngüsü

Siber tehdit istihbaratı, kurumların siber tehdit ortamını yalnızca teknik göstergeler üzerinden değil, tehdit aktörleri, saldırı motivasyonları, kullanılan taktikler, teknikler, prosedürler, hedeflenen varlıklar ve olası etkiler üzerinden anlamlandırmasını sağlayan sistematik bir güvenlik yaklaşımıdır. Bu yönüyle siber tehdit istihbaratı, yalnızca zararlı IP adresleri, alan adları, dosya hash değerleri veya zararlı bağlantılardan oluşan teknik gösterge listeleriyle sınırlı değildir. Teknik göstergeler, saldırının belirli bir anına veya belirli bir altyapı unsuruna işaret edebilir; ancak bu göstergelerin hangi tehdit aktörüyle ilişkili olduğu, hangi saldırı aşamasında kullanıldığı, hangi kurumsal varlıkları etkileyebileceği ve hangi savunma kararlarını gerektirdiği açıklanmadığında tek başına sınırlı değer üretir. Nist (2016) siber tehdit bilgisinin

kurumlar arasında paylaşılmasını ve operasyonel güvenlik süreçlerinde kullanılmasını, tehdit istihbaratı yönetiminin önemli bir bileşeni olarak ele almaktadır.

Bu nedenle CTI'nin temel işlevi, ham veriyi bağlamsal ve karar verilebilir bilgiye dönüştürmektir. Ham veri; log kayıtları, ağ trafiği, uç nokta alarmları, güvenlik ürünlerinden gelen bildirimler, zafiyet duyuruları, tehdit raporları, açık kaynak haberleri, karanlık web paylaşımları, sosyal medya sinyalleri, e-posta güvenliği kayıtları ve zararlı yazılım analiz çıktıları gibi çok farklı kaynaklardan gelebilir. Bu veriler tek başına dağınık, tekrar eden, eksik veya bağlamdan kopuk olabilir. Bilgi aşamasında bu veriler temizlenir, sınıflandırılır, zenginleştirilir ve anlamlı hâle getirilir. İstihbarat aşamasında ise bu bilgi, kurumun risk bağlamı içinde değerlendirilerek karar destek çıktısına dönüştürülür. Böylece "ne oldu?" sorusunun ötesine geçilerek "bu olay kurum için ne ifade ediyor?", "hangi varlıklar etkilenebilir?", "hangi öncelikle müdahale edilmelidir?" ve "hangi önleyici kontroller güçlendirilmelidir?" sorularına yanıt aranır.

Siber tehdit istihbaratı, kullanım amacı ve hedef kitlesine göre farklı seviyelerde ele alınmaktadır. Stratejik tehdit istihbaratı, üst yönetim, risk sahipleri ve karar vericiler için hazırlanır. Bu düzeyde amaç, kurumun içinde bulunduğu sektör, faaliyet gösterdiği coğrafya, iş modeli, regülasyon yükümlülükleri ve saldırgan motivasyonları dikkate alınarak uzun vadeli risk eğilimlerini açıklamaktır. Örneğin fidye yazılımı ekosistemindeki gelişmeler, tedarik zinciri saldırılarındaki artış, bulut güvenliği riskleri veya belirli sektörlere yönelen tehdit aktörleri stratejik istihbarat kapsamında değerlendirilebilir. Stratejik CTI, teknik ayrıntıdan çok yatırım öncelikleri, yönetim kararları, politika geliştirme ve

kurumsal risk yönetimi açısından önem taşır. SANS Institute (2025) tarafından yayımlanan CTI araştırması da stratejik, operasyonel ve taktik istihbaratın farklı karar düzeylerine hizmet ettiğini vurgulamaktadır.

Veri toplama aşamasında iç ve dış kaynaklardan tehdit verisi elde edilir. İç kaynaklar arasında SIEM kayıtları, EDR ve NDR telemetrisi, güvenlik duvarı logları, DNS sorguları, kimlik doğrulama kayıtları, e-posta güvenliği sistemleri, olay müdahale raporları ve varlık envanteri yer alır. Dış kaynaklar ise açık kaynak tehdit raporları, zafiyet veri tabanları, üretici güvenlik duyuruları, sektör paylaşım platformları, MISP gibi tehdit istihbaratı paylaşım sistemleri, karanlık web kaynakları ve ticari tehdit istihbaratı servislerinden oluşabilir. Bu aşamada yalnızca çok fazla veri toplamak değil, güvenilir, güncel, kurum bağlamına uygun ve doğrulanabilir veri kaynaklarını seçmek önemlidir. Bu veri paylaşım ve yapılandırma yaklaşımı, STIX ve TAXII gibi standartlarla teknik olarak desteklenmektedir (Oasis, 2021, 2021a, 2021b)

Sonuç olarak siber tehdit istihbaratı, kurumların siber tehditleri yalnızca teknik olaylar olarak değil, iş riski, saldırgan motivasyonu, savunma önceliği ve karar destek ihtiyacı açısından değerlendirmesini sağlayan stratejik bir güvenlik disiplinidir. Yapay zekâ bu disiplini daha hızlı, ölçeklenebilir ve bağlamsal hâle getirebilir; ancak bu katkı yalnızca iyi tanımlanmış istihbarat gereksinimleri, güvenilir veri kaynakları, insan denetimi ve ölçülebilir geri bildirim mekanizmalarıyla sürdürülebilir değer üretir. Siber tehdit istihbaratı türleri ve kullanım alanları Tablo 1’de sunulmuştur.

Tablo 1. Siber Tehdit İstihbaratı Türleri ve Kullanım Alanları

CTI Türü	**Hedef Kitle**	**Temel Kullanım**
Stratejik CTI	Üst yönetim ve risk sahipleri	Sektörel eğilimleri, saldırgan motivasyonlarını ve yatırım önceliklerini açıklar.
Operasyonel CTI	SOC ve olay müdahale ekipleri	Aktif kampanyaları, tehdit aktörlerini ve hedeflenen varlıkları değerlendirir.
Taktik CTI	Tehdit avcıları ve tespit mühendisleri	TTP, saldırı zinciri ve MITRE ATT&CK eşleştirmeleriyle savunmayı yönlendirir.
Teknik CTI	SIEM, EDR ve güvenlik araç ekipleri	IP, alan adı, URL, hash ve YARA/Sigma gibi göstergelerle hızlı aksiyon sağlar.

Yapay Zekânın CTI'deki Rolü ve Veri Ekosistemi

Yapay zekâ, siber tehdit istihbaratı süreçlerinde büyük hacimli, çok kaynaklı ve farklı formatlardaki güvenlik verilerinden anlamlı bilgi üretme kapasitesini artıran önemli bir teknolojik yaklaşımdır. Geleneksel CTI süreçlerinde analistler; tehdit raporları, güvenlik olay kayıtları, zararlı yazılım analizleri, açık kaynak verileri, zafiyet duyuruları, ağ trafiği kayıtları, uç nokta telemetrisi ve güvenlik ürünü alarmları gibi farklı kaynaklardan gelen bilgileri

manuel olarak incelemek zorunda kalmaktadır. Ancak günümüz tehdit ortamında veri hacminin artması, saldırı tekniklerinin çeşitlenmesi ve tehditlerin daha hızlı yayılması, manuel analiz kapasitesini zorlamaktadır. Bu nedenle yapay zekâ destekli yaklaşımlar, CTI süreçlerinde analistin karar verme hızını artıran, tekrar eden işleri azaltan, ilişkileri görünür kılan ve tehditleri önceliklendirmeye yardımcı olan bir karar destek katmanı olarak değerlendirilebilir. Yapay zekânın CTI süreçlerindeki bu rolü, siber güvenlikte üretken yapay zekâ ve makine öğrenmesi uygulamalarına ilişkin güncel çalışmalarla da desteklenmektedir (Balasubramanian vd., 2025; Mohamed, 2025).

Doğal dil işleme teknikleri, yapay zekâ destekli CTI'nin en önemli bileşenlerinden biridir. CTI süreçlerinde kullanılan verilerin önemli bir bölümü yapılandırılmamış metinlerden oluşmaktadır. Tehdit raporları, blog yazıları, güvenlik araştırmaları, zafiyet açıklamaları, üretici duyuruları, haber metinleri, sosyal medya paylaşımları, forum içerikleri ve karanlık web kaynakları farklı dillerde ve farklı anlatım biçimlerinde bilgi içerebilir. Doğal dil işleme yöntemleri bu metinlerden tehdit aktörü, zararlı yazılım ailesi, hedeflenen sektör, zafiyet kodu, ürün adı, saldırı tekniği, IP adresi, alan adı, URL ve dosya hash değeri gibi varlıkları otomatik olarak çıkarabilir. Bu sayede analistler, büyük hacimli metinleri tek tek okumak yerine önceden ayrıştırılmış, etiketlenmiş ve önceliklendirilmiş bilgi kümeleri üzerinden çalışabilir. Büyük hacimli tehdit raporlarından TTP çıkarımı yapılması, sistematik incelemelerde CTI otomasyonu açısından önemli bir kullanım alanı olarak ele alınmaktadır (Tamanna vd., 2026).

Büyük dil modelleri ve üretken yapay zekâ araçları, CTI raporlama ve analiz süreçlerinde giderek daha fazla

kullanılmaktadır. Bu modeller, uzun tehdit raporlarını özetleyebilir, teknik içeriği yönetici düzeyinde anlaşılır hâle getirebilir, olay kayıtlarından kronoloji çıkarabilir, analist notlarını rapor formatına dönüştürebilir ve belirli bir tehdit aktörü ya da saldırı tekniği hakkında ön analiz taslakları oluşturabilir. Ayrıca tehdit avcılığı senaryoları için hipotez üretme, SIEM sorgu taslakları hazırlama, Sigma veya YARA kuralı önerme ve olay müdahale adımlarını yapılandırma gibi alanlarda da destek sağlayabilir. Bununla birlikte üretken yapay zekâ çıktıları mutlak doğru kabul edilmemeli; kaynak doğrulaması, analist incelemesi ve teknik test süreçlerinden geçirilmelidir. Özellikle halüsinasyon, eksik bağlam ve yanlış kaynak üretimi gibi riskler nedeniyle bu modeller insan denetimli bir yardımcı araç olarak konumlandırılmalıdır. Üretken yapay zekâ çıktılarının doğrulanması, NIST AI RMF'de tanımlanan güvenilir ve sorumlu yapay zekâ yaklaşımıyla uyumludur (Nist, 2023).

Makine öğrenmesi, CTI süreçlerinde tehdit tespiti, sınıflandırma ve önceliklendirme için kullanılan temel yapay zekâ yaklaşımlarından biridir. Denetimli öğrenme modelleri, etiketlenmiş veri kümeleri üzerinden zararlı ve normal davranışları ayırt etmeyi öğrenebilir. Bu yaklaşım kimlik avı(phishing) e-postalarının sınıflandırılması, zararlı yazılım ailelerinin belirlenmesi, ağ trafiğinin normal veya şüpheli olarak ayrıştırılması ve güvenlik alarmlarının önceliklendirilmesi gibi alanlarda kullanılabilir. Denetimsiz öğrenme yöntemleri ise daha önce etiketlenmemiş verilerde benzerlikleri ve anormallikleri tespit etmek için değerlidir. Özellikle bilinmeyen saldırı örüntülerinin, olağan dışı kullanıcı davranışlarının, beklenmeyen ağ bağlantılarının veya benzer altyapı kullanan tehdit kampanyalarının belirlenmesinde denetimsiz öğrenme yaklaşımları CTI süreçlerine katkı sağlayabilir.

Yapay zekâ destekli risk skorlama, CTI çıktılarının operasyonel önceliklendirmeye dönüşmesinde kritik rol oynar. Her tehdit göstergesi veya zafiyet kurum açısından aynı düzeyde risk oluşturmaz. Bir zafiyetin CVSS skoru yüksek olabilir; ancak kurum envanterinde ilgili ürün bulunmuyorsa ya da sistem internete açık değilse önceliği farklı değerlendirilmelidir. Benzer şekilde kötü amaçlı olarak işaretlenen bir alan adı, kurum ağında hiç görülmemişse farklı; kritik bir sunucudan bu alan adına bağlantı tespit edilmişse çok daha farklı bir risk değerine sahiptir. Yapay zekâ destekli sistemler, tehdit göstergesi güvenilirliği, kaynak itibarı, aktif sömürü durumu, varlık kritiklik seviyesi, saldırı yüzeyi, gözlemlenen davranış ve iş etkisi gibi değişkenleri birlikte değerlendirerek önceliklendirilmiş risk skoru üretebilir.

Yapay zekâ destekli siber tehdit istihbaratı sistemlerinin başarısı, kullanılan veri kaynaklarının kapsamı, güvenilirliği, güncelliği ve kurumsal bağlamla ilişkilendirilebilme düzeyiyle doğrudan ilişkilidir. Siber tehdit istihbaratı, tek bir veri kaynağına dayanarak üretilebilecek basit bir güvenlik çıktısı değildir. Tehditlerin daha karmaşık, dağıtık ve çok aşamalı hâle gelmesi, farklı kaynaklardan gelen verilerin birlikte değerlendirilmesini zorunlu kılmaktadır. Bu nedenle CTI süreçlerinde iç güvenlik telemetrisi, açık kaynak istihbaratı, zafiyet veri tabanları, tehdit paylaşım platformları, karanlık web kaynakları, zararlı yazılım analizleri, DNS ve alan adı kayıtları, e-posta güvenliği verileri ve olay müdahale çıktıları birlikte ele alınmalıdır.

Veri kaynaklarının çeşitliliği CTI kalitesini artırma potansiyeline sahip olsa da bu durum aynı zamanda veri yönetimi zorluğunu da beraberinde getirir. Farklı kaynaklardan gelen veriler farklı formatlarda, farklı zaman dilimlerinde, farklı dil yapılarında

ve farklı güvenilirlik seviyelerinde olabilir. Bir kaynak JSON formatında yapılandırılmış IOC listesi sunarken, başka bir kaynak uzun bir tehdit raporu içinde serbest metin olarak bilgi sağlayabilir. Bazı kaynaklarda göstergeler güncel ve doğrulanmış olabilirken, bazı kaynaklarda eski, tekrar eden veya hatalı bilgiler bulunabilir. Bu nedenle yapay zekâ destekli CTI sistemlerinde ön işleme aşaması kritik öneme sahiptir.

Sonuç olarak yapay zekâ destekli siber tehdit istihbaratında veri kaynaklarının çeşitliliği önemli bir avantaj sağlasa da, bu avantaj ancak etkili ön işleme, güvenilirlik puanlama, normalleştirme, zenginleştirme, bağlamlandırma ve insan denetimiyle gerçek değere dönüşebilir. Kirli, eksik, doğrulanmamış veya bağlamdan kopuk veri, en gelişmiş yapay zekâ modelinde bile yanıltıcı sonuçlar üretebilir. Bu nedenle yapay zekâ destekli CTI mimarisinin temelinde yalnızca model seçimi değil, güçlü bir veri yönetişimi ve ön işleme yaklaşımı bulunmalıdır. Yapay zekâ tekniklerinin CTI'de kullanım alanları Tablo 2'de sunulmuştur. Bu nedenle veri kalitesi ve kaynak doğrulaması, yapay zekâ destekli CTI mimarisinin yalnızca teknik değil, yönetişim boyutunu da oluşturmaktadır (Nist, 2023, 2024).

Tablo 2. Yapay Zekâ Tekniklerinin CTI'de Kullanım Alanları

Yapay Zekâ Tekniği	**CTI'de Kullanım Alanı**	**Dikkat Edilecek Nokta**
Doğal Dil İşleme	Tehdit raporları ve zafiyet açıklamalarından IOC,	Dil ve bağlam hataları kaynak doğrulamasıyla azaltılmalıdır.

Yapay Zekâ Tekniği	CTI'de Kullanım Alanı	Dikkat Edilecek Nokta
	CVE, aktör ve teknik çıkarımı yapar.	
Büyük Dil Modelleri	Rapor özetleme, olay kronolojisi, analist notu ve yönetici özeti üretir.	Halüsinasyon ve hassas veri riski nedeniyle insan kontrolü gerekir.
Makine Öğrenmesi	Phishing sınıflandırma, IOC skorlama ve alarm önceliklendirme sağlar.	Başarı veri kalitesi, etiketleme ve güncelliğe bağlıdır.
Graf Analitiği	Aktör, altyapı, IOC, zafiyet ve TTP ilişkilerini görünür kılar.	Eksik ilişki verileri yanlış bağlantı kurulmasına neden olabilir.
Otomasyon/SOAR	Alarm zenginleştirme, playbook, bilet ve olay özeti üretir.	Yanlış pozitiflerde otomatik aksiyon sınırlandırılmalıdır.

IOC, IoA, TTP ve MITRE ATT&CK Eşleştirme

Siber tehdit istihbaratında tehdit göstergelerinin doğru yorumlanabilmesi için IOC, IoA ve TTP kavramlarının birbirinden ayrılması önemlidir. Bu kavramlar çoğu zaman aynı güvenlik olayının farklı düzeylerini ifade eder. IOC daha çok saldırının teknik izlerine, IoA saldırı davranışına, TTP ise saldırganın izlediği yöntem ve süreçlere odaklanır. Yapay zekâ destekli CTI sistemlerinin yalnızca teknik göstergeleri toplaması yeterli değildir; bu göstergeleri davranışsal bağlama yerleştirmesi, saldırı zinciriyle ilişkilendirmesi ve kurumsal savunma kontrolleriyle eşleştirmesi gerekir.

IOC, yani uzlaşma göstergeleri, bir sistemde veya ağda zararlı faaliyetin gerçekleşmiş olabileceğini gösteren teknik izlerdir. IP adresleri, alan adları, URL'ler, dosya hash değerleri, zararlı e-posta adresleri, komuta-kontrol sunucuları, dosya adları, registry anahtarları ve belirli imza örüntüleri IOC kapsamında değerlendirilebilir. IOC'ler güvenlik operasyonları açısından hızlı aksiyon üretme potansiyeline sahiptir. Örneğin zararlı olduğu doğrulanan bir alan adı güvenlik duvarında engellenebilir, bir dosya hash değeri EDR sisteminde karantinaya alınabilir veya bilinen bir zararlı IP adresi SIEM korelasyon kuralına eklenebilir.

IoA, yani saldırı göstergeleri, teknik göstergelerden ziyade saldırgan davranışına odaklanır. IoA; olağan dışı komut çalıştırma örüntüleri, beklenmeyen yetki yükseltme girişimleri, olağan dışı kimlik doğrulama davranışları, şüpheli süreç zincirleri, komut satırı parametreleri, lateral movement işaretleri, veri sızdırma davranışları veya anormal ağ bağlantıları gibi davranışsal belirtileri kapsar.

TTP kavramı, saldırganların kullandığı taktik, teknik ve prosedürleri ifade eder. Taktik, saldırganın ulaşmak istediği genel amacı; teknik, bu amaca ulaşmak için kullandığı yöntemi; prosedür ise yöntemin belirli bir olay veya kampanya içinde nasıl uygulandığını gösterir. Örneğin kimlik bilgisi elde etmek bir taktik amaca, phishing e-postası göndermek bir tekniğe, belirli bir kurumun çalışanlarına yönelik özelleştirilmiş sahte giriş sayfası kullanmak ise prosedüre örnek olarak verilebilir. TTP yaklaşımı, saldırgan davranışını daha kalıcı ve savunma açısından daha anlamlı bir düzeyde ele alır.

MITRE ATT&CK çerçevesi, saldırgan taktik ve tekniklerini ortak bir dil ile ifade etmeyi sağlayan en yaygın kullanılan yapılardan biridir. ATT&CK, saldırı yaşam döngüsünün farklı

aşamalarında kullanılan teknikleri sınıflandırarak güvenlik ekiplerinin tehditleri daha sistematik biçimde analiz etmesine olanak tanır. Bu çerçeve; tehdit istihbaratı, tehdit avcılığı, tespit mühendisliği, olay müdahale, kırmızı takım faaliyetleri, savunma boşluk analizi ve güvenlik kontrol değerlendirmesi gibi birçok alanda kullanılabilir. Al-Sada vd. (2024) gerçekleştirdikleri çalışmada MITRE ATT&CK'in tehdit modelleme, tespit mühendisliği ve savunma boşluk analizi açısından yaygın kullanılan bir çerçeve olduğunu belirtmektedir; güncel ATT&CK bilgi tabanı da bu tekniklerin ortak bir sınıflandırma diliyle sunulmasını sağlamaktadır (Mitre, 2026).

Sonuç olarak IOC, IoA ve TTP ayrımı, siber tehdit istihbaratının teknik veri listesinden davranışsal ve karar destek odaklı bir yapıya dönüşmesi açısından temel öneme sahiptir. IOC'ler hızlı aksiyon üretirken, IoA'lar saldırı davranışını anlamayı, TTP'ler ise saldırgan yöntemlerini daha kalıcı biçimde modellemeyi sağlar. MITRE ATT&CK eşleştirmesi bu kavramları ortak bir dil altında birleştirerek CTI çıktılarının tehdit avcılığı, tespit mühendisliği, olay müdahale ve savunma olgunluğu değerlendirmesi süreçlerinde kullanılmasını kolaylaştırır. Yapay zekâ ise bu eşleştirme ve ilişkilendirme süreçlerini hızlandırabilir; ancak model çıktılarının analist doğrulamasıyla desteklenmesi, güvenilir ve sürdürülebilir CTI üretimi için zorunludur. IOC, IoA ve TTP kavramlarının karşılaştırılması Tablo 3'te sunulmuştur. Ayrıca IOC'den TTP'ye bağlamsallaştırma akışı Şekil 2'de gösterilmiştir. TTP çıkarımı ve ATT&CK eşleştirmesi, yapay zekâ destekli CTI çalışmalarında otomasyon potansiyeli yüksek alanlar arasında değerlendirilmektedir (Tamanna vd., 2026).

Tablo 3. IOC, IoA ve TTP Kavramlarının Karşılaştırılması

Kavram	**Odak Noktası ve Örnekler**	**CTI Açısından Değer / Sınırlılık**
IOC	IP, alan adı, URL, hash ve zararlı e-posta adresi gibi teknik izlere odaklanır.	Hızlı tespit sağlar; ancak kolay değiştiği için bağlamla birlikte kullanılmalıdır.
IoA	Şüpheli komut, yetki yükseltme, lateral movement ve olağan dışı davranışlara odaklanır.	Bilinmeyen saldırıları yakalayabilir; güçlü davranış analizi gerektirir.
TTP	Kimlik avı, kalıcılık, komuta-kontrol ve veri sızdırma gibi saldırgan yöntemlerini açıklar.	Daha kalıcı savunma değeri üretir; doğru eşleştirme analist uzmanlığı ister.
MITRE ATT&CK	Taktik ve teknikleri ortak sınıflandırma diliyle düzenler.	SOC, tehdit avcılığı ve olay müdahale ekipleri arasında ortak dil sağlar.

Şekil 2. IOC'den TTP'ye Bağlamsallaştırma Akışı

Yapay Zekâ Destekli Kullanım Senaryoları ve CTI Standartları

Yapay zekâ destekli siber tehdit istihbaratı, yalnızca kuramsal bir yaklaşım değil, güvenlik operasyonlarının birçok aşamasında uygulanabilir somut kullanım senaryoları sunan pratik bir güvenlik kapasitesidir. CTI süreçlerinde yapay zekânın değeri; veri toplama, ön işleme ve analiz aşamalarının ötesinde, kurumun gerçek güvenlik problemlerine uygulanabildiğinde ortaya çıkar. Bu nedenle yapay zekâ destekli CTI kullanım senaryoları, güvenlik operasyon merkezi faaliyetleri, olay müdahale süreçleri, zafiyet yönetimi, tehdit avcılığı, zararlı yazılım analizi, kimlik avı tespiti, risk önceliklendirme ve otomatik raporlama gibi alanlarla doğrudan ilişkilidir.

Yapay zekâ destekli CTI'nin en yaygın kullanım alanlarından biri kimlik avı saldırılarının tespitidir. Kimlik avı saldırıları, kullanıcıları sahte bağlantılara yönlendirme, zararlı ek dosya açtırma, kimlik bilgisi toplama veya ödeme dolandırıcılığı gerçekleştirme amacıyla kullanılmaktadır. Geleneksel e-posta güvenliği yaklaşımları gönderen adresi, alan adı itibarı, imza tabanlı zararlı dosya kontrolü ve bilinen URL listeleri üzerinden tespit yaparken; yapay zekâ destekli sistemler e-posta metni, dil yapısı, sosyal mühendislik kalıpları, bağlantı özellikleri, ek dosya davranışı, gönderen geçmişi ve kullanıcı etkileşimi gibi farklı değişkenleri birlikte analiz edebilir. Bu sayede yalnızca bilinen phishing göstergeleri değil, daha önce görülmemiş ancak davranışsal olarak şüpheli e-posta örüntüleri de tespit edilebilir.

Örneğin yüksek CVSS skoruna sahip bir zafiyet, kurumda kullanılmayan bir ürünü etkiliyorsa operasyonel önceliği düşük olabilir. Buna karşılık orta seviyeli bir zafiyet, internete açık kritik bir sistemde bulunuyor, exploit kodu kamuya açık şekilde yayımlanmış ve tehdit aktörleri tarafından aktif olarak kullanılıyorsa öncelik seviyesi yüksek olmalıdır. Yapay zekâ destekli risk skorlama modelleri, bu çok boyutlu bağlamı analiz ederek yama yönetimi ekiplerine daha uygulanabilir bir aksiyon sıralaması sunabilir. Bu yaklaşım, zafiyet yönetimi ile CTI arasında güçlü bir bağ kurar. Zafiyetlerin yalnızca teknik ciddiyetle değil, kurumsal bağlamla birlikte değerlendirilmesi gerektiğinden CVSS v4.0 puanlama yaklaşımı bu süreçte temel referanslardan biri olarak kullanılabilir (FIRST, 2023).

Tehdit avcılığında yapay zekânın katkısı yalnızca sorgu üretimiyle sınırlı değildir. Makine öğrenmesi ve anomali tespiti modelleri, kurum ortamında normal davranıştan sapan kullanıcı,

cihaz, süreç veya ağ bağlantısı örüntülerini belirleyebilir. Örneğin bir kullanıcının olağan çalışma saatleri dışında farklı ülkelerden oturum açması, daha önce erişmediği sistemlere erişim denemesi, kısa sürede çok sayıda dosya indirmesi veya olağan dışı komutlar çalıştırması davranışsal risk sinyali olarak değerlendirilebilir. Bu tür sinyaller CTI bağlamıyla birlikte ele alındığında tehdit avcılığı daha hedefli ve etkili hâle gelir.

Bu kullanım senaryosu, CTI'nin teknik göstergeden davranışsal istihbarata geçişini destekler. Örneğin aynı zararlı yazılım ailesinin farklı hash değerlerine sahip varyantları olabilir; ancak dosya davranışları, ağ iletişimi ve kalıcılık yöntemleri benzerlik gösterebilir. Yapay zekâ destekli kümelendirme, bu benzerlikleri ortaya çıkararak tehdit aktörü ilişkilendirmesi, kampanya analizi ve savunma kuralı üretimi açısından değerli bilgiler sağlayabilir. Bununla birlikte zararlı yazılım analizi modellerinin sandbox kaçınma teknikleri, eksik davranış gözlemi ve hatalı etiketleme gibi sınırlılıkları dikkate alınmalıdır.

Siber tehdit istihbaratının kurumsal güvenlik süreçlerinde etkili biçimde kullanılabilmesi için üretilen bilginin ortak bir dil, standart veri formatları ve güvenilir paylaşım mekanizmaları üzerinden yönetilmesi gerekir. CTI yalnızca kurum içinde üretilen raporlardan veya teknik gösterge listelerinden oluşmaz; farklı güvenlik araçları, kurumlar, sektör toplulukları, araştırmacılar ve istihbarat platformları arasında paylaşılabilir, ilişkilendirilebilir ve otomasyona uygun hâle getirilebilir bir yapıya ihtiyaç duyar. Bu nedenle CTI platformları, standartlar ve çerçeveler; tehdit bilgisinin toplanması, yapılandırılması, analiz edilmesi, paylaşılması ve operasyonel aksiyona dönüştürülmesi açısından kritik öneme sahiptir. STIX ve TAXII standartları, CTI verisinin yapılandırılmış

biçimde ifade edilmesi ve güvenilir taraflar arasında otomatik paylaşılması için yaygın kullanılan temel mekanizmalardır (Oasis 2021, 2021a, 2021b).

MITRE ATT&CK, saldırganların gerçek dünyada gözlemlenen taktik, teknik ve prosedürlerini sınıflandıran bir bilgi tabanıdır. CTI bağlamında ATT&CK'in en önemli katkısı, saldırgan davranışının standart bir yapı içinde ifade edilmesini sağlamasıdır. Bu yapı sayesinde tehdit raporlarında geçen davranışlar, güvenlik alarmları, olay müdahale bulguları ve tehdit avcılığı hipotezleri ortak bir sınıflandırmaya bağlanabilir. Örneğin bir saldırı olayında kimlik bilgisi toplama, yetki yükseltme, savunmadan kaçınma veya komuta-kontrol iletişimi gibi davranışlar ATT&CK teknikleriyle eşleştirildiğinde, yalnızca olay açıklaması yapılmış olmaz; aynı zamanda kurumun bu tekniklere karşı tespit ve önleme kapasitesi de değerlendirilebilir. Bu nedenle ATT&CK eşleştirmesi, CTI çıktılarının SOC, tehdit avcılığı ve olay müdahale süreçlerinde ortak bir dil üzerinden kullanılmasına katkı sağlar (Al-Sada vd., 2024; Mitre, 2026).

MISP, tehdit göstergelerinin ve olay bilgilerinin paylaşılması için kullanılan önemli CTI platformlarından biridir. MISP benzeri paylaşım platformları, kurumların IOC, tehdit aktörü, zararlı yazılım, kampanya, zafiyet ve olay bilgilerini yapılandırılmış biçimde kaydetmesine, ilişkilendirmesine ve paylaşmasına olanak tanır. Bu tür platformlar, kurum içi CTI süreçlerinin yanı sıra sektörler arası iş birliği, topluluk temelli tehdit paylaşımı ve olay müdahale koordinasyonu açısından da değerlidir. Özellikle aynı sektörde faaliyet gösteren kurumlar benzer tehditlerle karşılaşabildiği için güvenilir paylaşım toplulukları erken uyarı ve kolektif savunma açısından önemli katkı sağlayabilir.

Sonuç olarak CTI platformları, standartlar ve çerçeveler, yapay zekâ destekli siber tehdit istihbaratının kurumsal güvenlik süreçlerine entegre edilmesinde temel rol oynar. MITRE ATT&CK saldırgan davranışının ortak dil ile tanımlanmasını, MISP tehdit göstergelerinin bağlamlı paylaşımını, STIX/TAXII yapılandırılmış veri aktarımını, CVSS zafiyet ciddiyetinin değerlendirilmesini, NIST ve ISO çerçeveleri ise bu bilgilerin kurumsal risk yönetimiyle bütünleştirilmesini sağlar. Yapay zekâ bu yapıların üzerinde hızlandırıcı ve ilişkilendirici bir katman olarak konumlandırıldığında, CTI süreçleri daha ölçeklenebilir, bağlamsal ve operasyonel olarak uygulanabilir hâle gelir. Yapay zekâ Destekli CTI kullanıma senaryoları da Tablo 4'te sunulmuştur. Bu bütünleşik yaklaşım; ATT&CK, STIX/TAXII, CVSS ve NIST CSF gibi çerçevelerin birlikte kullanılmasını gerektirir (First, 2023; Mitre, 2026; Nist, 2024; Oasis, 2021a, 2021b).

Tablo 4. Yapay Zekâ Destekli CTI Kullanım Senaryoları

Kullanım Senaryosu	**Üretilen CTI Çıktısı**	**Operasyonel Katkı**
Kimlik avı tespiti	Phishing risk skoru, şüpheli URL ve ek dosya değerlendirmesi	Kullanıcı hedefli saldırıların erken tespitini sağlar.
Zafiyet önceliklendirme	Kurum bağlamına göre sıralanmış CVE ve yama önerisi	Yama sırasını gerçek risk düzeyine göre belirler.
Tehdit avcılığı	Avcılık hipotezi, ATT&CK eşleştirmesi ve SIEM/EDR sorgusu	Gizli tehditlerin proaktif aranmasını sağlar.

Kullanım Senaryosu	Üretilen CTI Çıktısı	Operasyonel Katkı
Zararlı yazılım analizi	Aile, kampanya ve davranışsal TTP ilişkisi	Hash tabanlı yaklaşımın ötesinde davranışsal istihbarat üretir.
SOAR otomasyonu	Olay özeti, bilet, playbook ve önerilen aksiyon	Müdahale süresini kısaltır ve operasyonel tutarlılığı artırır.

Açıklanabilir Yapay Zekâ, Güvenilirlik ve Risk Yönetimi

Yapay zekâ destekli siber tehdit istihbaratı sistemlerinin güvenlik operasyonlarında etkili biçimde kullanılabilmesi için yalnızca doğru sonuç üretmesi yeterli değildir. Modelin hangi veriye dayanarak hangi sonucu ürettiğinin anlaşılabilir olması, karar sürecinin izlenebilmesi ve gerektiğinde insan analist tarafından doğrulanabilmesi gerekir. Siber güvenlik gibi yüksek riskli bir alanda yapay zekâ çıktıları; alarm önceliklendirme, zafiyet yönetimi, tehdit avcılığı, otomatik engelleme, olay müdahale ve yönetici raporlaması gibi kritik süreçlere etki edebilir. Bu nedenle yapay zekâ destekli CTI sistemlerinde açıklanabilirlik, güvenilirlik ve denetlenebilirlik temel tasarım ilkeleri arasında yer almalıdır. Açıklanabilirlik ve hesap verebilirlik, NIST AI RMF'de güvenilir yapay zekâ sistemlerinin temel özellikleri arasında konumlandırılmaktadır (Nist, 2023).

Açıklanabilir yapay zekâ, modelin ürettiği sonucun insanlar tarafından anlaşılabilir gerekçelerle desteklenmesini ifade eder. CTI bağlamında bu gereklilik daha da önemlidir; çünkü bir tehdidin neden yüksek riskli olarak değerlendirildiği, bir IOC'nin neden

önceliklendirildiği, bir olayın hangi ATT&CK tekniğiyle ilişkilendirildiği veya bir zafiyetin neden acil kapatılması gerektiği açık biçimde ifade edilmelidir. “Model bu alarmı yüksek riskli buldu” ifadesi güvenlik operasyonu için yeterli değildir. Bunun yerine modelin; göstergenin güvenilir bir kaynakta yer aldığını, kurum içinde kritik bir varlıkla ilişkilendiğini, aktif saldırı kampanyasında kullanıldığını, belirli bir saldırı tekniğiyle eşleştiğini veya geçmiş olaylarla benzerlik gösterdiğini açıklaması gerekir.

Açıklanabilirlik, analist güveni açısından kritik bir unsurdur. SOC analistleri, tehdit avcıları ve olay müdahale ekipleri, model çıktılarının gerekçesini göremediğinde bu çıktılara güvenmekte zorlanabilir. Özellikle yanlış pozitif oranının yüksek olduğu güvenlik ortamlarında, açıklama sunmayan bir model kısa sürede operasyonel yükü artıran bir araca dönüşebilir. Buna karşılık açıklanabilir CTI sistemleri, analistin modeli daha etkin kullanmasını sağlar. Analist, yalnızca sonuca değil, sonuca götüren göstergelere, kaynaklara ve ilişkilere bakarak daha bilinçli karar verebilir.

Büyük dil modellerinin CTI süreçlerinde kullanılması açıklanabilirlik konusunu daha da önemli hâle getirmektedir. Büyük dil modelleri uzun tehdit raporlarını özetleyebilir, teknik metinleri sadeleştirebilir, olay kronolojisi oluşturabilir, IOC ve TTP çıkarımı yapabilir veya yönetici raporu taslağı hazırlayabilir. Ancak bu modeller halüsinasyon üretebilir; yani kaynak metinde bulunmayan bilgileri varmış gibi sunabilir. Ayrıca teknik terimleri yanlış yorumlayabilir, kaynakları karıştırabilir veya kesin olmayan bilgileri kesinmiş gibi ifade edebilir. Bu nedenle LLM tabanlı CTI çıktıları kaynak metinle karşılaştırılmalı, alıntılanan göstergeler doğrulanmalı ve kritik kararlar öncesinde analist kontrolünden

geçirilmelidir. LLM tabanlı CTI çıktılarında halüsinasyon ve kaynak doğrulama sorunları, üretken yapay zekânın siber güvenlikteki temel sınırlılıkları arasında gösterilmektedir (Balasubramanian vd., 2025; Mohamed, 2025).

Sonuç olarak açıklanabilir yapay zekâ ve güvenilir CTI, yapay zekâ destekli siber tehdit istihbaratının sürdürülebilir biçimde kullanılabilmesi için temel gerekliliklerdir. Modelin ne sonuç ürettiği kadar, bu sonucu nasıl ürettiği, hangi kaynağa dayandığı, hangi güven düzeyine sahip olduğu ve hangi insan denetimiyle doğrulandığı da önemlidir. Yapay zekâ destekli CTI sistemleri; açıklanabilirlik, kaynak doğrulama, insan onayı, veri kalitesi, mahremiyet, denetlenebilirlik ve geri bildirim ilkeleriyle tasarlandığında güvenlik operasyonlarına gerçek değer sağlayabilir. Aksi hâlde yapay zekâ, CTI süreçlerini güçlendirmek yerine yanlış pozitifleri, hatalı önceliklendirmeleri ve operasyonel riskleri artıran bir unsur hâline gelebilir.

Yapay zekâ destekli siber tehdit istihbaratı sistemleri, güvenlik operasyonlarına hız, ölçeklenebilirlik, ilişkilendirme ve karar desteği açısından önemli katkılar sunmakla birlikte, yeni risk alanları da oluşturmaktadır. Bu riskler yalnızca modelin teknik doğruluğu ile sınırlı değildir. Veri kalitesi, kaynak güvenilirliği, model dayanıklılığı, mahremiyet, mevzuat uyumu, açıklanabilirlik, otomasyona aşırı güven, adversarial saldırılar, veri zehirleme, model hırsızlığı ve insan denetiminin zayıflaması gibi birçok unsur yapay zekâ destekli CTI sistemlerinin güvenilirliğini etkileyebilir. Bu nedenle yapay zekâ destekli CTI, yalnızca performans ve hız odaklı değil, risk temelli ve denetlenebilir bir yaklaşımla tasarlanmalıdır. Bu risk temelli yaklaşım, hem yapay zekâ risk yönetimi hem de

kurumsal siber güvenlik yönetişimi çerçeveleriyle uyumludur (Nist, 2023, 2024).

Veri kalitesi sorunu özellikle IOC tabanlı tehdit istihbaratında belirginleşmektedir. Eski bir alan adı, daha önce kötü amaçlı kullanılmış bir IP adresi veya bağlamdan kopuk bir hash değeri yanlış şekilde yüksek riskli olarak sınıflandırılabilir. Bu durumda güvenlik araçları gereksiz alarm üretebilir veya meşru iletişimler engellenebilir. Benzer şekilde eksik veri nedeniyle gerçekten kritik bir tehdit düşük öncelikli değerlendirilebilir. Bu nedenle yapay zekâ destekli CTI sistemlerinde veri temizleme, tekrar yönetimi, güncellik kontrolü, kaynak itibarı ve kurum içi gözlem bilgisi birlikte değerlendirilmelidir.

Mahremiyet riski yalnızca dış servislere veri gönderimiyle sınırlı değildir. Kurum içinde çalışan bir model de gereğinden fazla kişisel veya hassas veriye erişirse yetkisiz kullanım, yetki aşımı veya iç tehdit riskleri ortaya çıkabilir. Bu nedenle yapay zekâ destekli CTI sistemlerinde rol tabanlı erişim kontrolü, veri sınıflandırma, yetki ayrımı, iz kayıtları ve denetim mekanizmaları uygulanmalıdır. Analistin ihtiyaç duyduğu bilgi ile modelin işleyebileceği veri arasında amaçla sınırlılık ilkesi korunmalıdır.

Sonuç olarak yapay zekâ destekli CTI sistemleri, kurumların tehditleri daha hızlı anlamasına ve güvenlik operasyonlarını daha proaktif hâle getirmesine yardımcı olabilir. Ancak bu sistemler veri kalitesi sorunları, veri zehirleme, adversarial saldırılar, halüsinasyon, mahremiyet ihlalleri, model önyargısı, yanlış pozitifler, otomasyona aşırı güven ve denetlenebilirlik eksikliği gibi riskler barındırmaktadır. Bu nedenle yapay zekâ destekli CTI yaklaşımı, insan denetimi, açıklanabilirlik, kaynak doğrulama, güvenli otomasyon, veri yönetişimi ve sürekli izleme ilkeleriyle

birlikte tasarlanmalıdır. Yapay zekâ, kontrolsüz bir otomasyon aracı değil, güvenilir ve denetlenebilir bir karar destek bileşeni olarak konumlandırıldığında CTI süreçlerine sürdürülebilir değer sağlayabilir. Yapay zekâ destekli CTI riskleri ve azaltım stratejileri Tablo 5'te sunulmuştur. Bu nedenle yüksek etkili güvenlik aksiyonlarında insan onayı, kaynak doğrulama ve geri alma mekanizmaları korunmalıdır (Nist, 2023; Mohamed, 2025).

Tablo 5. Yapay Zekâ Destekli CTI Riskleri ve Azaltım Stratejileri

Risk Alanı	**Olası Etki**	**Azaltım Stratejisi**
Veri kalitesi sorunu	Hatalı istihbarat ve yanlış önceliklendirme üretir.	Temizleme, normalleştirme, kaynak puanlama ve kurum içi doğrulama yapılmalıdır.
Veri zehirleme	Modelin yanlış öğrenmesine veya manipüle edilmesine neden olabilir.	Çoklu kaynak doğrulama ve analist onayı uygulanmalıdır.
Adversarial saldırı	Tehditlerin normal davranış gibi sınıflandırılmasına yol açabilir.	Dayanıklılık testleri, davranışsal analiz ve sürekli güncelleme kullanılmalıdır.
Halüsinasyon	Olmayan IOC, yanlış CVE yorumu veya hatalı rapor üretebilir.	Kaynak bağlantılı çıktı ve insan doğrulaması zorunlu tutulmalıdır.
Mahremiyet riski	KVKK/GDPR ihlali ve hassas veri sızıntısı doğurabilir.	Maskeleme, anonimleştirme, erişim kontrolü ve veri

Risk Alanı	Olası Etki	Azaltım Stratejisi
		minimizasyonu uygulanmalıdır.
Otomasyona aşırı güven	Yanlış pozitiflerde iş sürekliliği riski oluşturabilir.	Yüksek etkili aksiyonlarda insan onayı ve geri alma planı korunmalıdır.

Kurumsal Uygulama Modeli ve Önerilen Mimari

Yapay zekâ destekli siber tehdit istihbaratının kurumsal düzeyde değer üretebilmesi için yalnızca teknik bir araç olarak değil, veri yönetişimi, güvenlik operasyonları, risk yönetimi, olay müdahale ve insan denetimiyle bütünleşik bir yapı olarak ele alınması gerekir. Kurumlar yapay zekâ destekli CTI yaklaşımını uygularken öncelikle hangi güvenlik problemini çözmek istediklerini belirlemelidir. Bu problem; alarm yorgunluğunu azaltmak, zafiyet önceliklendirmeyi iyileştirmek, phishing saldırılarını daha hızlı tespit etmek, tehdit avcılığı hipotezleri üretmek, tehdit raporlarını özetlemek veya SOAR entegrasyonuyla olay müdahalesini hızlandırmak olabilir. Uygulama modeli, kurumun güvenlik olgunluğu ve mevcut teknolojik altyapısı dikkate alınarak aşamalı biçimde tasarlanmalıdır. Kurumsal uygulama modeli tasarlanırken NIST CSF 2.0'ın yönetişim, risk yönetimi ve sürekli iyileştirme yaklaşımı ile NIST AI RMF'nin yapay zekâ risk yönetimi ilkeleri birlikte değerlendirilebilir (Nist, 2023, 2024).

Önerilen kurumsal mimarinin ilk katmanı veri kaynaklarıdır. Bu katmanda SIEM kayıtları, EDR ve NDR telemetrisi, güvenlik duvarı logları, DNS kayıtları, e-posta güvenliği verileri, zafiyet

tarama sonuçları, varlık envanteri, MISP gibi tehdit istihbaratı paylaşım platformları, açık kaynak tehdit raporları, CVE veri tabanları, üretici güvenlik duyuruları ve olay müdahale raporları yer alır. Bu kaynaklar, kurum içi gözlem ile dış tehdit bilgisinin birlikte değerlendirilmesini sağlar. Bu katmanda kurum içi telemetri ile dış CTI kaynaklarının birlikte ele alınması, NIST SP 800-150'de vurgulanan tehdit bilgisi paylaşımı yaklaşımıyla uyumludur (Nist, 2016).

İkinci katman veri işleme ve normalleştirme katmanıdır. Farklı kaynaklardan gelen veriler farklı formatlarda, farklı zaman damgalarıyla ve farklı güvenilirlik düzeyleriyle üretilebilir. Bu nedenle verilerin temizlenmesi, tekrar eden kayıtların ayıklanması, IOC ve CVE gibi varlıkların ayrıştırılması, kaynak güvenilirliğinin puanlanması ve kurum varlık envanteriyle ilişkilendirilmesi gerekir. Bu katman, yapay zekâ modellerinin doğru ve bağlamsal sonuç üretebilmesi için kritik öneme sahiptir.

Beşinci katman risk skorlama ve karar destek katmanıdır. Bu katmanda model çıktıları kurum bağlamıyla birlikte değerlendirilir. Risk skoru oluşturulurken göstergenin kaynak güvenilirliği, aktif saldırı kampanyasında kullanılıp kullanılmadığı, kurum içinde görülme durumu, etkilenen varlığın kritiklik seviyesi, internete açıklık, saldırı zincirindeki konum ve mevcut güvenlik kontrolleri dikkate alınır. Böylece CTI çıktısı yalnızca "zararlı" veya "temiz" şeklinde ikili bir karar üretmez; öncelik, güven düzeyi, gerekçe ve önerilen aksiyon ile birlikte sunulur.

Önerilen mimaride insan denetimi merkezi bir rol üstlenir. Yapay zekâ sistemleri analiste öneri, özet, sınıflandırma, risk skoru ve aksiyon taslağı sunabilir; ancak nihai karar özellikle yüksek riskli durumlarda insan uzmanlığıyla doğrulanmalıdır. Bu nedenle yapay

zekâ destekli CTI mimarisi “insan dışı otomasyon” değil, “insan denetimli karar destek” modeli olarak tasarlanmalıdır.

Sonuç olarak kurumsal düzeyde uygulanabilir bir yapay zekâ destekli CTI modeli; çok kaynaklı veri toplama, ön işleme, zenginleştirme, yapay zekâ analizi, risk skorlama, operasyonel entegrasyon ve insan denetimi bileşenlerinden oluşmalıdır. Bu model, kurumların tehditleri daha hızlı anlamasına, kritik riskleri önceliklendirmesine ve güvenlik operasyonlarını daha proaktif hâle getirmesine yardımcı olabilir. Ancak bu değer, yalnızca doğru veri yönetişimi, açıklanabilir model çıktıları, ölçülebilir başarı kriterleri ve kontrollü otomasyon ilkeleriyle sürdürülebilir hâle gelir. Kurumsal yapay zekâ destekli CTI uygulama aşamaları Tablo 6’da gösterilmiştir. Böylece yapay zekâ destekli CTI, yalnızca teknik otomasyon değil; yönetişim, risk yönetimi, standartlaştırma ve insan denetimiyle desteklenen sürdürülebilir bir karar destek modeli hâline gelir (Nist, 2023, 2024).

Tablo 6. Kurumsal yapay zekâ Destekli CTI Uygulama Aşamaları

Aşama	**Temel Amaç**	**Beklenen Çıktı**
İhtiyaç analizi	Phishing veya tehdit avcılığı gibi CTI önceliklerini belirlemek.	Kapsamı tanımlanmış kullanım senaryosu.
Veri hazırlığı	SIEM, EDR, DNS, MISP ve varlık envanterini temizleyip ilişkilendirmek.	Normalleştirilmiş ve güvenilir veri seti.
Pilot uygulama	Sınırlı alanda model çıktısını ve analist geri bildirimini test etmek.	Ölçülebilir performans ve iyileştirme listesi.

Aşama	Temel Amaç	Beklenen Çıktı
Entegrasyon	CTI çıktısını SIEM/SOAR, bilet ve olay yönetimi süreçlerine aktarmak.	Operasyonel karar destek akışı.
İnsan denetimi	Kritik aksiyonlarda analist onayı ve hesap verebilirlik sağlamak.	Güvenli ve kontrollü otomasyon.
Ölçüm ve iyileştirme	Yanlış pozitif, müdahale süresi ve analist memnuniyetini izlemek.	Sürekli iyileştirilen CTI modeli.

Kaynakça

Al-Sada, B., Sadighian, A., & Oligeri, G. (2024). Mitre att&ck: State of the art and way forward. ACM Computing Surveys, 57(1), Article 12. https://doi.org/10.1145/3687300

Balasubramanian, P., Liyanage, S., Sankaran, H., Sivaramakrishnan, S., Pusuluri, S., Pirttikangas, S., & Peltonen, E. (2025). Generative AI for cyber threat intelligence: Applications, challenges, and analysis of real-world case studies. Artificial Intelligence Review, 58(11), Article 336. https://doi.org/10.1007/s10462-025-11371-y

Brown, R., & Sfakianakis, A. (2025, May 20). SANS 2025 CTI survey webcast & forum: Navigating uncertainty in today's threat landscape. SANS Institute. https://www.sans.org/white-papers/2025-cti-survey-webcast-forum-navigating-uncertainty-todays-threat-landscape

First. (2023). Common vulnerability scoring system version 4.0: Specification document. Forum of Incident Response and Security Teams. https://www.first.org/cvss/v4.0/specification-document

Mitre. (2026). Mitre att&ck. https://attack.mitre.org/

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems, 67(8), 6969–7055. https://doi.org/10.1007/s10115-025-02429-y

Nist. (2016). National institute of standards and technology .Guide to cyber threat information sharing (Nist Special Publication 800-150). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-150

Nist. (2023). National institute of standards and technology. Artificial Intelligence Risk Management Framework (Ai Rmf 1.0) (Nist Ai 100-1). U.S. Department of commerce. https://doi.org/10.6028/NIST.AI.100-1

Nist. (2024). National institute of standards and technology. The Nist cybersecurity framework (Csf) 2.0 (Nist Cswp 29). U.S. Department of commerce. https://doi.org/10.6028/NIST.CSWP.29

Oasis. (2021). Stix v2.1 and Taxii v2.1 Oasis standards are published. https://www.oasis-open.org/2021/06/23/stix-v2-1-and-taxii-v2-1-oasis-standards-are-published/

Oasis. (2021a). Stix version 2.1. Oasis Open. https://oasis-open.github.io/cti-documentation/

Oasis. (2021b). Taxii version 2.1. Oasis Open. https://www.oasis-open.org/standard/taxii-version-2-1/

Tamanna, M., Mitra, S., Erfan, M., Ryan, A., Mittal, S., Williams, L., & Rahman, M. R. (2026). What are adversaries doing? Automating tactics, techniques, and procedures extraction: A systematic review. arXiv. https://doi.org/10.48550/arXiv.2604.02377


BİDGE