İMMUNE PROGRAMMİNG

BAĞIŞIKLIK SİSTEMİ TABANLI PROGRAMLAMA

Giriş (Introduction)

- ***Yapay zeka (Artificial Intelligence) nedir?***
- ***Yapay zeka, bilgisayar sistemlerinin insan zekasına özgü öğrenme, akıl yürütme, problem çözme ve karar verme gibi bilişsel işlevleri taklit edebilmesini amaçlayan bir bilim ve mühendislik alanıdır. Bu alanda geliştirilen birçok yöntem, doğadan ve biyolojik sistemlerden ilham alır. Bu yaklaşımlardan biri olan Immune Programming (Bağışıklık Programlama), insan bağışıklık sisteminin öğrenme, tanıma ve adaptasyon yeteneklerini temel alarak geliştirilmiş bir yapay zeka tekniğidir. Özellikle optimizasyon, anomali tespiti ve siber güvenlik gibi alanlarda etkili çözümler sunar***

Immune Programming Nedir?

- ***Immune Nedir?***
- ***Immune (Bağışıklık), canlı organizmaların vücuda giren yabancı maddeleri tanıma, bu maddelere karşı savunma geliştirme ve kendini koruma yeteneğidir. İnsan bağışıklık sistemi; tanıma, öğrenme, çoğalma ve adaptasyon gibi karmaşık süreçlerle çalışır.***
- ***Immune Programming***
- ***İnsan bağışıklık sisteminin bu karmaşık süreçlerini algoritmalarla taklit eden bir YAPAAY ZEKA yöntemidir. Bu yöntem, özellikle optimizasyon, anomali tespiti ve sınıflandırma gibi alanlarda kullanılır. Ayrıca, dinamik ve değişken ortamlarda kendini geliştirebilme özelliği sayesinde SİBER GÜVENLİKTE saldırı tespiti ve tehdit analizi gibi kritik uygulamalarda da etkin olarak kullanılır.***

Yapay Bağışıklık Sistemleri (Artificial Immune Systems - AIS)

- **Yapay Bağışıklık Sistemleri (AIS), biyolojik bağışıklık sisteminin çalışma prensiplerinden ilham alınarak geliştirilmiş yapay zeka teknikleridir. İnsan vücudunun, zararlı yabancı maddeleri tanıyıp onlara karşı savunma geliştirmesi gibi, AIS de bilgisayar sistemlerinde anormallik tespiti, öğrenme ve adaptasyon gibi işlevleri yerine getirir.**

AIS’in Gelişimi ve Özellikleri

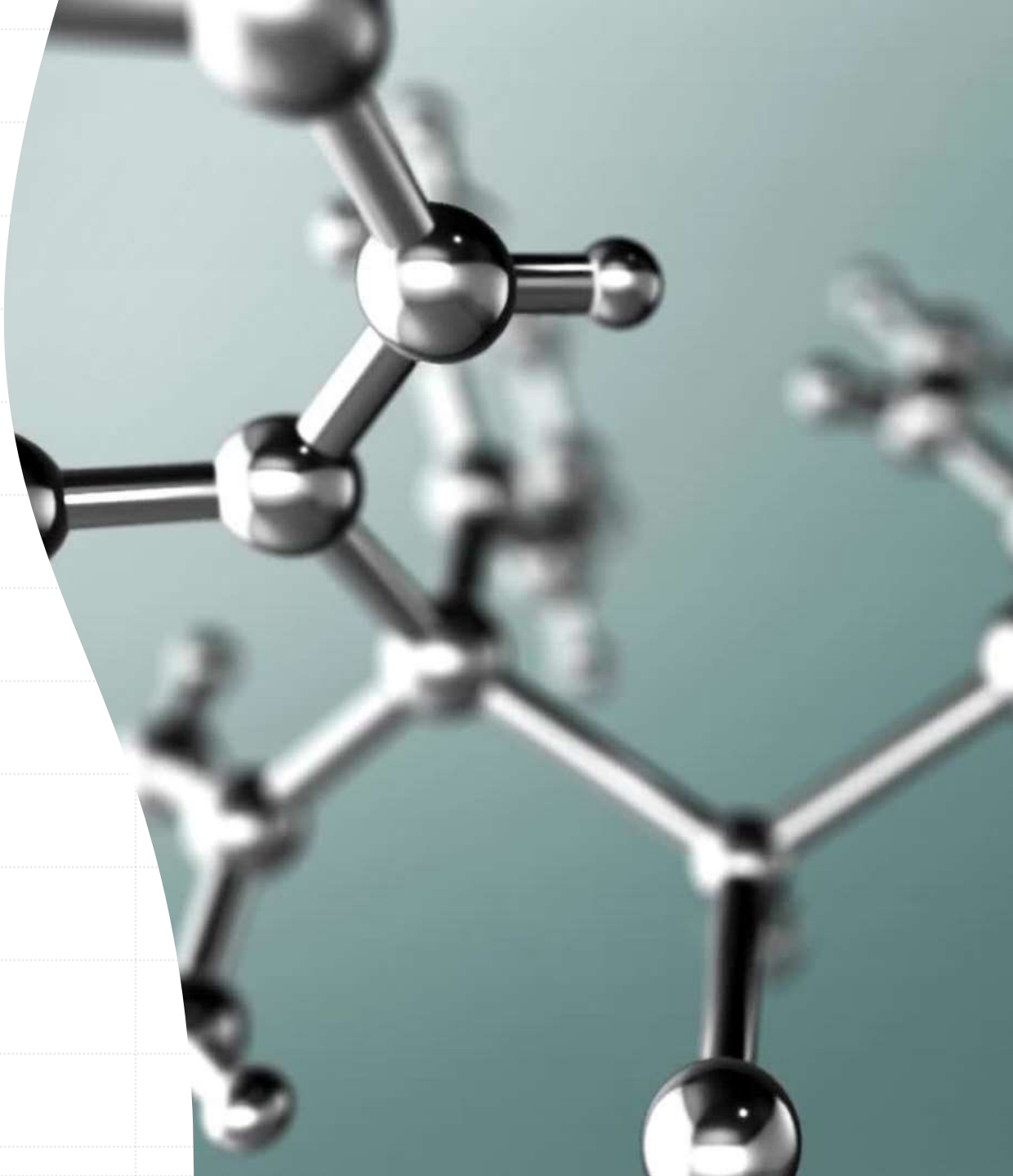
- **AIS, 1990’lı yılların başında bilgisayar bilimciler tarafından biyolojik bağışıklık sisteminin karmaşık ve etkili koruma mekanizmalarının yapay ortama uyarlanması fikriyle ortaya çıkmıştır. İlk çalışmalar arasında, Forrest ve arkadaşlarının (1994) geliştirdiği Negative Selection Algorithm önemli bir yer tutar; bu algoritma, normal davranışları öğrenerek anormal durumları tespit etmeye dayanır.**
- **Daha sonra, AIS alanı, de Castro ve Timmis (2002) gibi araştırmacılar sayesinde, bağışıklık ağları, klonal seçilim ve dendritik hücre algoritması gibi farklı biyolojik mekanizmaların yapay modellerini içerecek şekilde genişlemiştir. AIS, özellikle adaptasyon, gürültüye dayanıklılık ve dinamik ortamlarda etkinlik gibi avantajları nedeniyle siber güvenlik, optimizasyon ve sınıflandırma gibi alanlarda yaygın olarak kullanılır.**

Yapay Bağışıklık Sistemi Algoritmaları

- **Yapay Bağışıklık Sistemleri, insan bağışıklık sisteminin çalışma şeklinden esinlenerek geliştirilmiş algoritmalardır. Bu algoritmalar, bilgisayarların karmaşık verileri analiz edip öğrenmesini sağlar. Özellikle siber güvenlikte, bilinmeyen saldırıları tespit etmek için kullanılırlar.**

Kullanılan Temel Algoritmalar

- ***Negative Selection Algorithm (NSA)***
- ***Clonal Selection Algorithm (CSA)***
- ***Immune Network Algorithm***
- ***Dendritic Cell Algorithm (DCA)***



Negative Selection Algorithm (NSA)

- Yapay bağışıklık sistemlerinin en temel algoritmalarından biridir ve insan bağışıklık sisteminin “kendini-yabancıdan ayırma” (self–nonself discrimination) yeteneğini taklit eder. Bilgisayar sistemlerinde, normal (self) davranışları öğrenir ve bunlardan farklı olanları (non-self) **anormal** ya da **potansiyel tehdit** olarak tanımlar.

⚙ Çalışma Prensibi:

- **Self Set (Kendi Verisi) Tanımlama:**
  Sistemin normal çalışmasına ait veriler alınır. Bu veriler sistemin “kendi”sidir.
- **Detektörlerin Rastgele Oluşturulması:**
  Rastgele veri örneklerinden oluşan bir detektör havuzu oluşturulur.
- **Negatif Seçilim (Eğitim):**
  Detektörler, self verilerle karşılaştırılır. Eğer bir detektör self veriye benziyorsa el edilir, çünkü sistemin normalini tehdit olarak algılamaması gerekir.
- **Tespit (Uygulama):**
  Kalan detektörler artık anormal davranışları tespit etmek için kullanılır. Bir veri örneği self verilerle eşleşmiyorsa ve bir detektörle eşleşiyorsa anomali olarak etiketlenir.

- ***Siber Güvenlikte Kullanımı:***
- **Anomali Tespiti:**
  Bilinmeyen saldırıların veya zararlı aktivitelerin tespitinde güçlüdür.
- **Ağ Güvenliği:**
  Normal ağ trafiği öğrenildikten sonra, olağandışı veya şüpheli trafik davranışları (örneğin DDoS, port tarama, brute force saldırıları) kolaylıkla tespit edilebilir.
- Antivirüs / IDS Sistemleri:
  Kötü amaçlı yazılımın veya şüpheli sistem faaliyetlerinin belirlenmesinde kullanılır.

Avantajları:

- Bilinmeyen saldırıları da tespit edebilir (diğer klasik yöntemlere göre üstün).
- Biyolojik olarak ilham aldığı için doğası gereği adaptiftir.
- Gürültülü verilerle başa çıkabilir.

Dezavantajları:

- Detektör üretimi ve eşleştirme süreçleri büyük veri kümelerinde zaman alabilir.
- Self alanının doğru tanımlanmaması, yanlış alarmlara neden olabilir

Clonal Selection Algorithm (CSA)

Bağışıklık sisteminin antijenlere karşı en etkili yanıtları üretme sürecini taklit eder. İnsan vücudu, bir yabancı maddeye karşı etkili olan antikorları seçip çoğaltır ve bunları mutasyona uğratarak çeşitlendirir. CSA, bu biyolojik süreci **optimizasyon**, **öğrenme** ve **örüntü tanıma** gibi alanlara uygulamak için geliştirilmiştir.

⚙ Çalışma Prensibi:

- **Girdi Popülasyonu Oluşturulur:**
  Rastgele çözümler (antikorlar gibi) bir popülasyon oluşturur.
- **En İyi Adayların Seçilmesi:**
  Popülasyondaki en iyi çözümler seçilir (fitness değerine göre).
- **Klonlama:**
  Seçilen çözümler, başarı düzeyleriyle orantılı olarak klonlanır. Yani iyi çözümler daha fazla çoğaltılır.
- **Mutasyon:**
  Klonlar, küçük değişikliklerle mutasyona uğratılır. Amaç, çözümleri çeşitlendirerek daha iyilerini bulmaktır.
- **Seçim ve Yenileme:**
  Klonlar ve orijinal bireyler değerlendirilir. En iyi olanlar korunur, diğerleri yeni rastgele çözümlerle değiştirilir.
- **Döngü:**
  Bu işlem belirli sayıda tekrar edilir ya da durma koşulu sağlanana kadar devam eder.

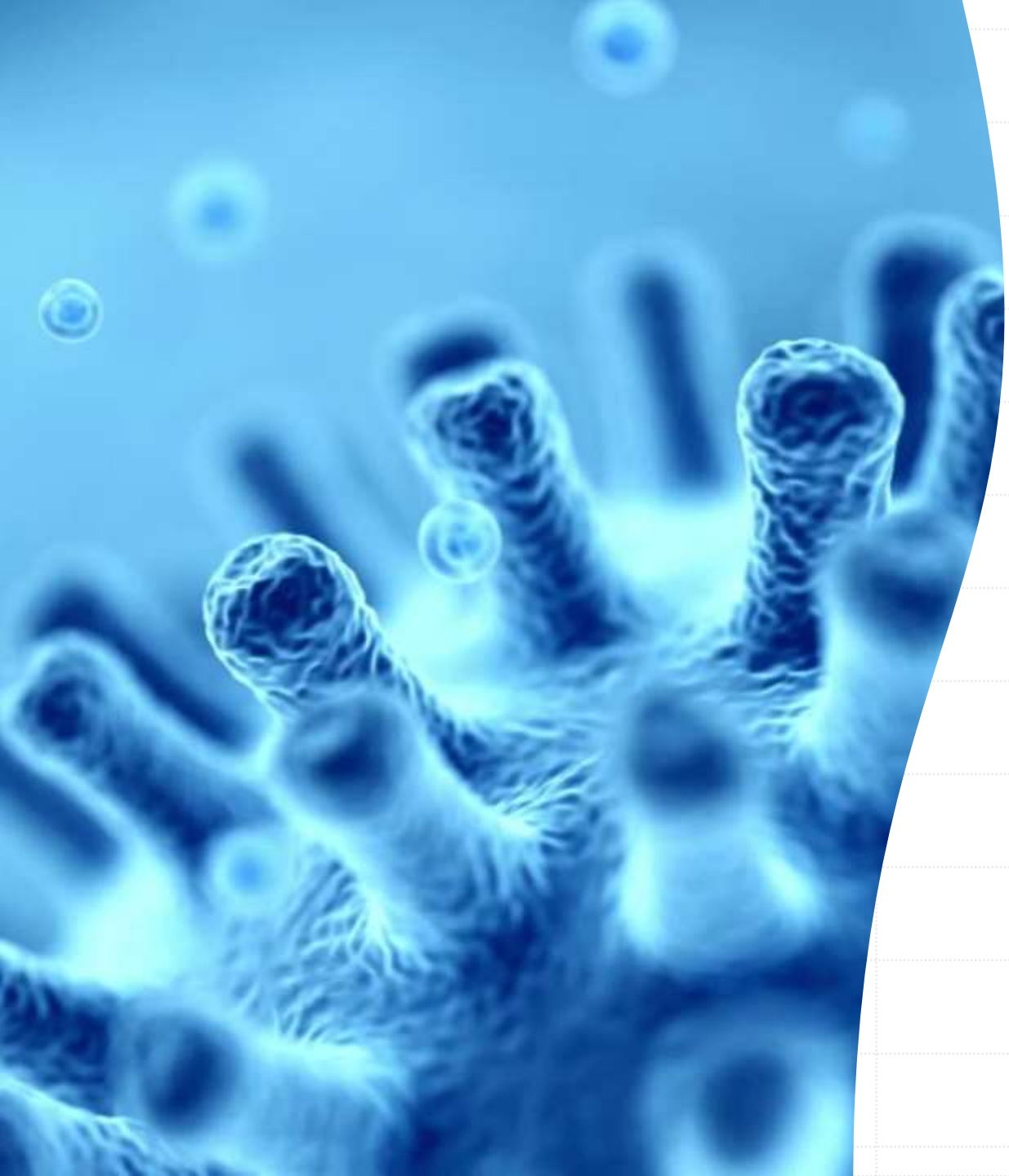
- 🛡️ **Siber Güvenlikte Kullanımı:**
- **Kötü Amaçlı Yazılım Sınıflandırması:**
  Farklı zararlı yazılım türlerinin otomatik olarak tanınmasında kullanılır.
- **Öznitelik Seçimi:**
  Saldırı tespiti sistemlerinde, veriden en anlamlı özellikleri seçmek için kullanılır.
- **Güvenlikte Optimizasyon:**
  Güvenlik politikalarının ya da sistem ayarlarının en uygun hale getirilmesinde (örneğin kaynak kullanımı ile güvenlik düzeyini dengelemede) uygulanabilir.

Avantajları:

- Karmaşık problemlere güçlü optimizasyon yeteneği sunar.
- Adaptif bir yapıya sahiptir (dinamik sistemlere uygundur).
- Lokal optimumlara sıkışmayı azaltır (mutasyon sayesinde).

Dezavantajları:

- Çok sayıda klonlama ve mutasyon işlemi hesaplama maliyetini artırabilir.
- Parametre ayarları (klon sayısı, mutasyon oranı) iyi yapılmazsa etkisiz sonuçlar üretebilir.



Immune Network Algorithm (INA)

Immune Network Algorithm (Bağışıklık Ağı Algoritması), bağışıklık sisteminde bulunan antikorların yalnızca antijenlere değil, **birbirlerine de tepki verdiği** gerçeğine dayanır. Bu etkileşimler sonucunda, sistem **öğrenme**, **hafıza** ve **örüntü tanıma** gibi yetenekler kazanır.

INA, bu biyolojik mekanizmayı modelleyerek, **veriler arasında ilişkileri öğrenen ve kendini güncelleyen bir yapay bağışıklık ağı** oluşturur.

⚙ Çalışma Prensibi:

- **Başlangıç Popülasyonu (Antikorlar):**
  Rasgele antikor örneklerinden oluşan bir başlangıç kümesi oluşturulur.
- **Antijen ile Eşleşme:**
  Antijen sisteme sunulur. Uygun antikorlar, bu antijene karşı uyarılır.
- **Etkileşim Ağı Kurulması:**
  Antikorlar yalnızca antijenle değil, birbirleriyle de benzerliğe göre etkileşime girer.
  Güçlü benzerlik ilişkileri bağ kurar, zayıf olanlar sistemden çıkarılır.
- **Klonlama ve Mutasyon:**
  Uyarılan antikorlar klonlanır ve mutasyona uğratılır.
- **Ağ Güncelleme:**
  Yeni antikorlar ağa eklenir; zayıf, eski ya da tekrar edenler silinir. Sistem sürekli güncellenir ve öğrenir.

- □ Siber Güvenlikte Kullanımı:
- **Ağ Trafiği Davranış Modelleme:**
  Kullanıcı davranışlarını temsil eden antikorlar oluşturularak, bu davranışlar zamanla izlenebilir ve şüpheli faaliyetler fark edilebilir.
- **Gelişmiş Anomali Tespiti:**
  Antikorlar arası etkileşim sayesinde çok boyutlu, karmaşık saldırı örüntüleri tespit edilebilir**.**
- **Adaptif Saldırı Tespiti:**
  Sistem, yeni tehditler karşısında kendini güncelleyerek daha güçlü hale gelir.
-

Avantajları:

- Bellek ve öğrenme yeteneği sağlar (sistem zamanla daha iyi hale gelir).
- Karmaşık örüntüleri tanıma kapasitesi yüksektir.
- Adaptiftir, değişen saldırı türlerine karşı tepki verebilir.

Dezavantajları:

- Ağı yönetmek ve güncellemek işlem gücü ister.
- Uygulama karmaşıklığı diğer algoritmalara göre daha fazladır.

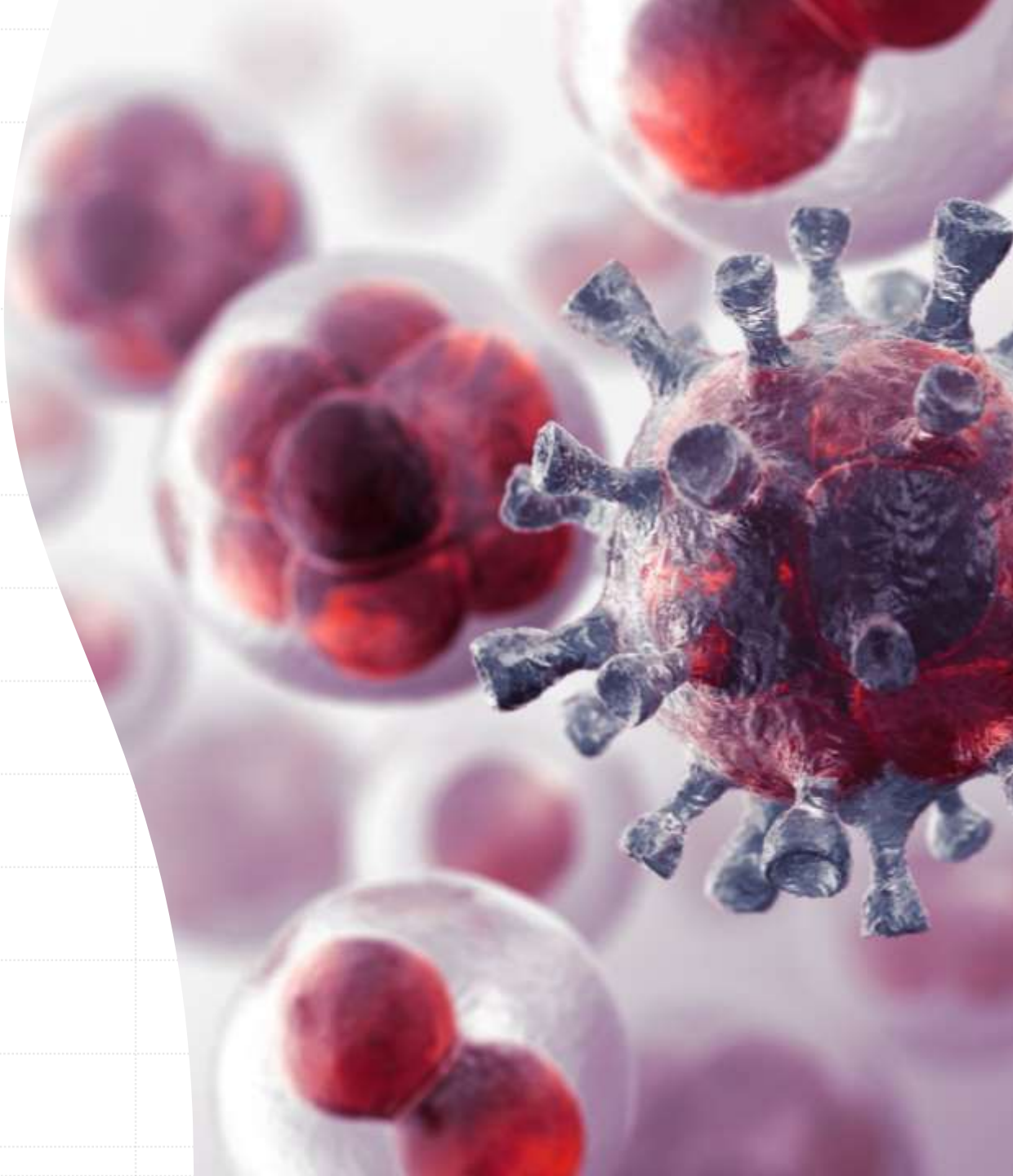
Dendritic Cell Algorithm (DCA)

▪Dendritic Cell Algorithm, bağışıklık sistemindeki **dendritik hücrelerin** çalışma şeklinden esinlenerek geliştirilmiş bir algoritmadır. Bu hücreler, vücuttaki sinyalleri (tehlike, güvenlik, bağlam vs.) toplayarak hangi durumların tehdit içerdiğine karar verir.

- DCA, aynı bu biyolojik süreci taklit ederek **birden fazla veri sinyalini değerlendirip**, olayları **normal ya da anormal** olarak sınıflandırır. Bu özelliğiyle özellikle **siber güvenlikte çok boyutlu anomali tespiti** için güçlü bir yöntemdir.

▪⚙ Çalışma Prensibi:

- **Girdi Sinyalleri Tanımlanır:**
  - Danger signals (tehlike sinyalleri)
  - Safe signals (güvenli sinyaller)
  - Pathogen Associated Molecular Patterns – PAMPs (zararlı sinyaller)
    Sistem, bu sinyalleri dış dünyadan (örneğin ağ trafiği, işlem süresi, veri akışı) alır.
- **Dendritik Hücrelerin Oluşturulması:**
  Hücreler, gelen sinyalleri toplayarak bir karar verir:
  "Bu durum zararlı mı, değil mi?"
- **Kontekst Kararı (Sınıflandırma):**
  - Eğer tehlike sinyalleri baskınsa → **Anomalidir.**
  - Eğer güvenli sinyaller fazlaysa → **Normaldir.**
    Her hücre birden fazla sinyali değerlendirerek bu kararı verir.
- **Hafıza Oluşturma:**
  Zamanla sistem, hangi özelliklerin anormal olduğunu daha iyi öğrenir ve kararlarını buna göre günceller.



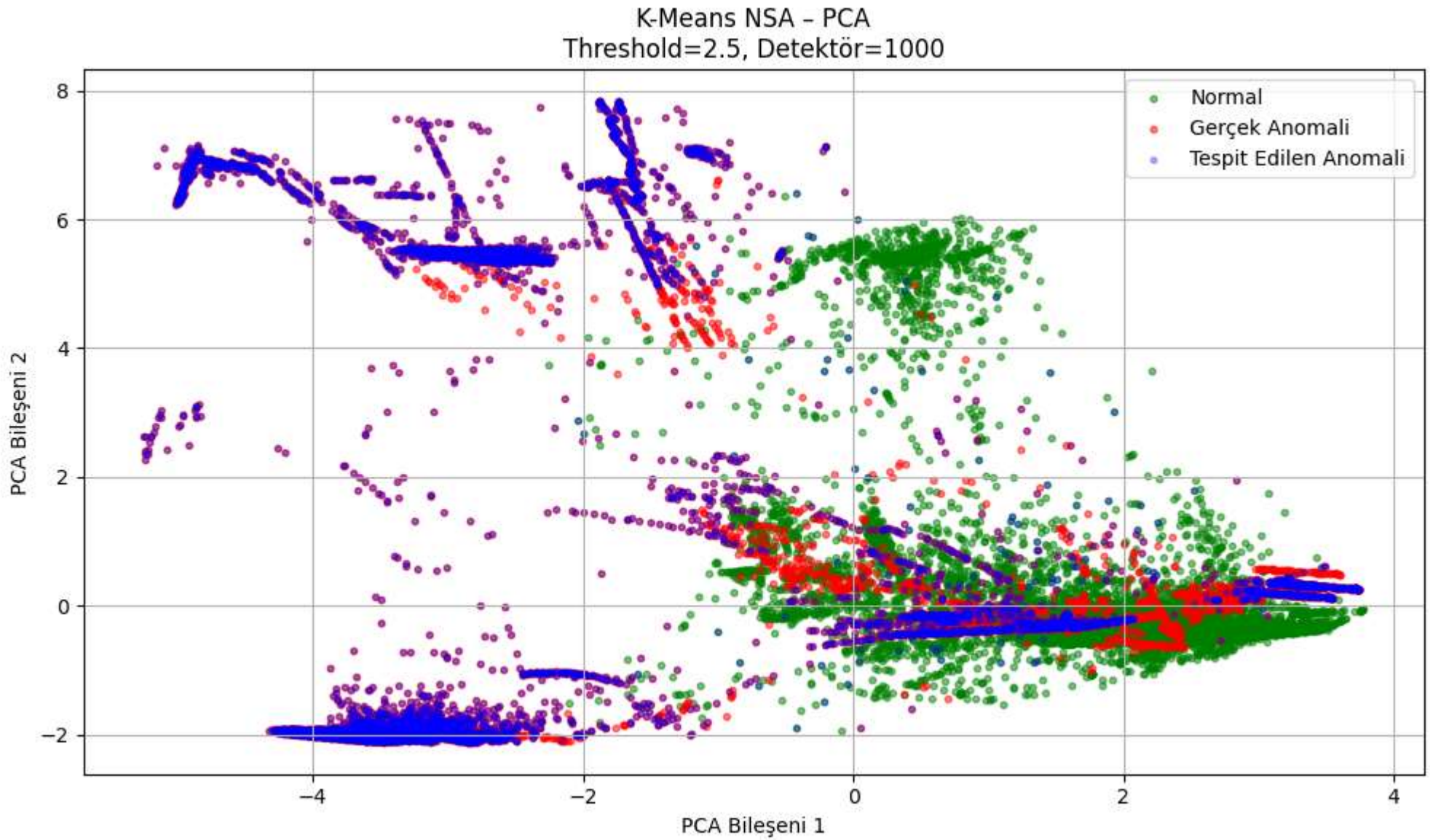
- □ Siber Güvenlikte Kullanımı:
- **Ağ Anomali Tespiti:**
  Farklı trafik özelliklerini (paket hızı, bağlantı sıklığı, veri boyutu vs.) analiz ederek saldırı davranışlarını tespit eder.
- **Gelişmiş IDS (Intrusion Detection System) Sistemleri:**
  Özellikle çoklu sinyal kaynağının olduğu ortamlarda etkilidir.
- **Davranış Analizi:**
  Kullanıcı veya sistem davranışları zamana yayılmış şekilde incelenir ve tehdit oluşturabilecek örüntüler tespit edilir.

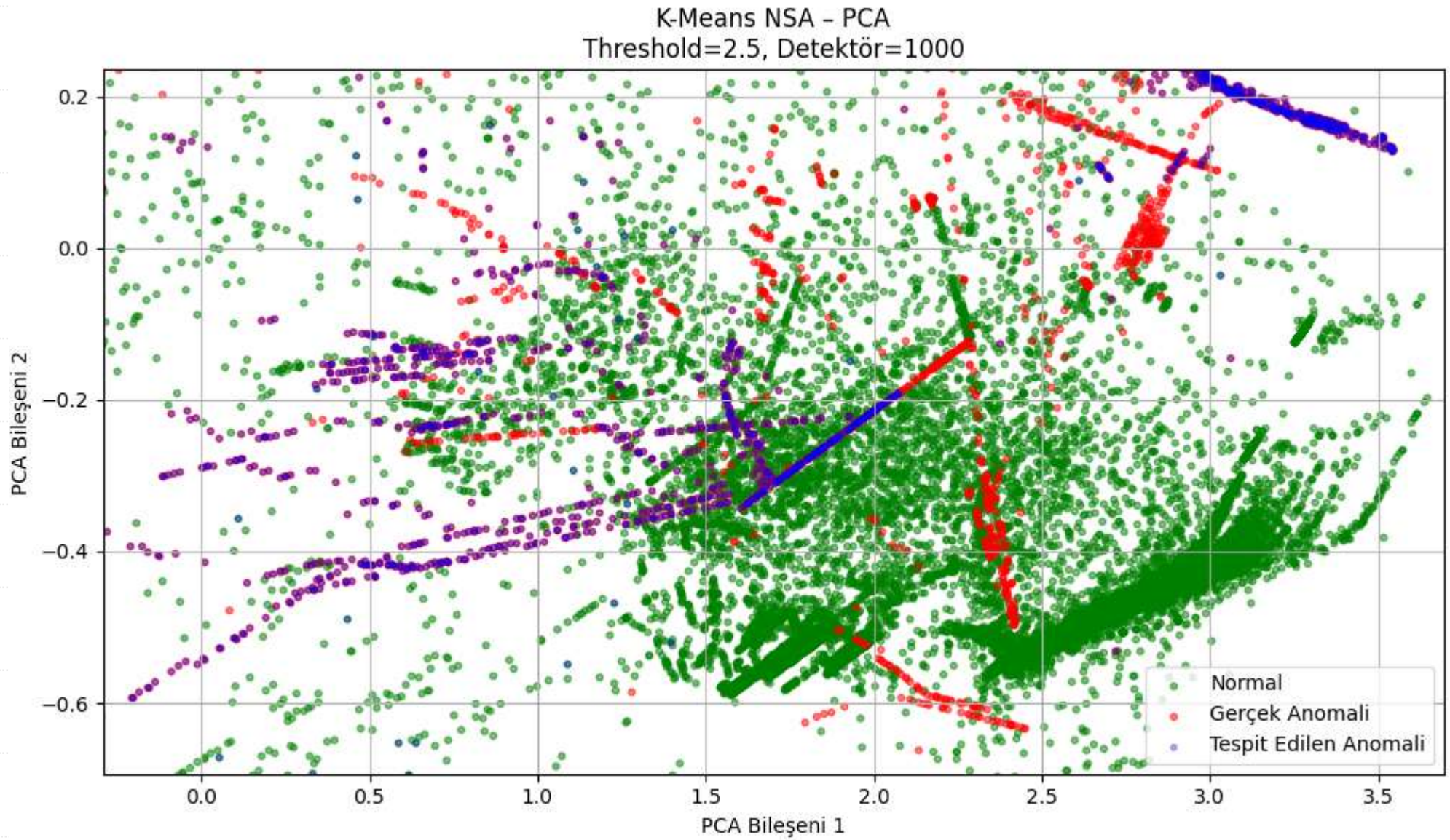
Avantajları:

- Çok sayıda sinyali aynı anda analiz edebilir.
- Gerçek dünyadaki saldırı örüntülerine daha yakındır.
- Dinamik sistemlerde yüksek doğruluk sağlar.

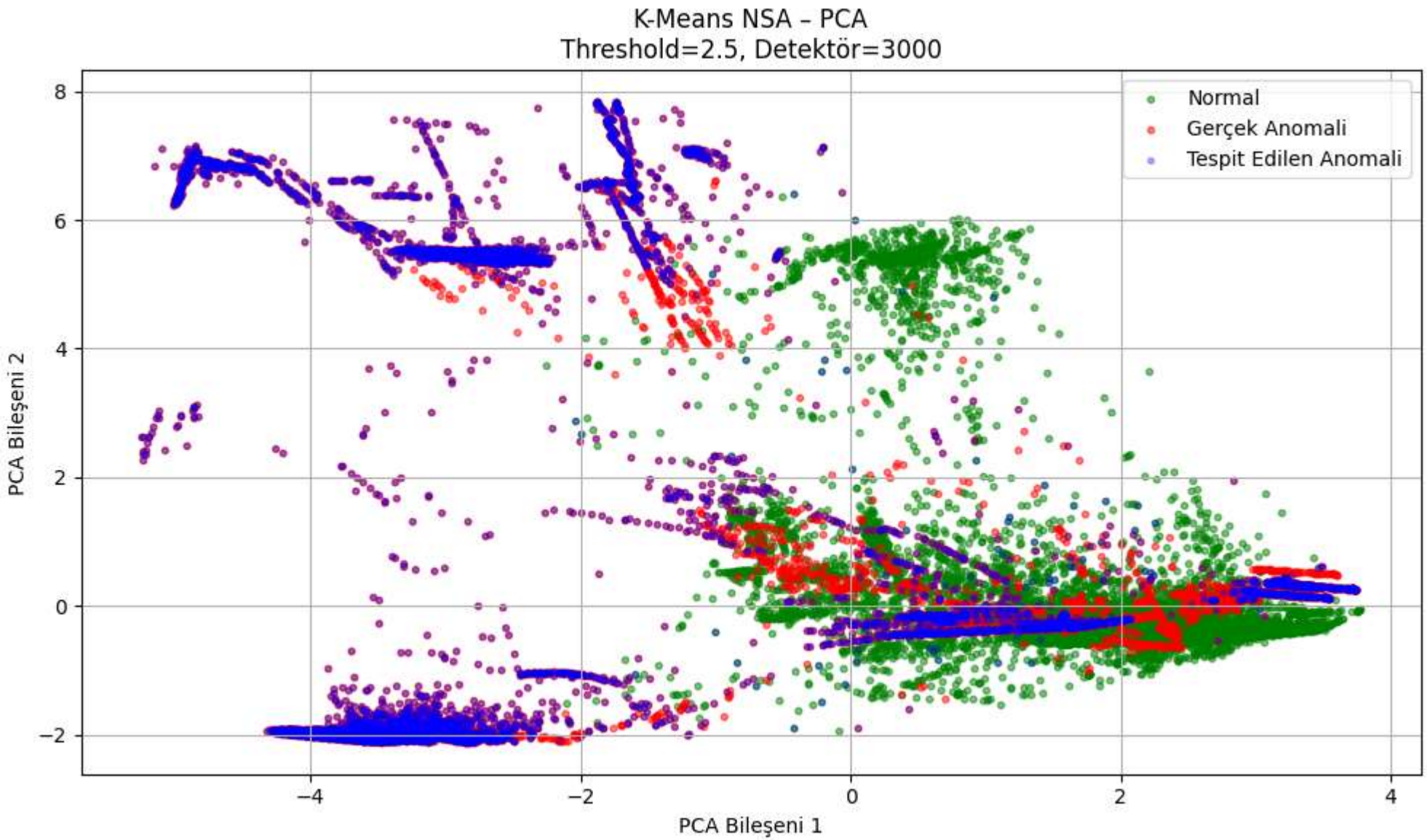
Dezavantajları:

- Parametre ayarı karmaşıktır.
- Uygulaması ve test süreci zaman alabilir.
- Farklı sinyallerin doğru şekilde sınıflandırılması gerekir.


K-Means NSA – PCA
Threshold=2.5, Detektör=1000
Normal
Gerçek Anomali
Tespit Edilen Anomali
PCA Bileşeni 1
PCA Bileşeni 2
8
6
4
2
0
−2
−4
−2
0
2
4


K-Means NSA – PCA
Threshold=2.5, Detektör=1000
PCA Bileşeni 2
PCA Bileşeni 1
0.2
0.0
−0.2
−0.4
−0.6
0.0
0.5
1.0
1.5
2.0
2.5
3.0
3.5
Normal
Gerçek Anomali
Tespit Edilen Anomali

```
=== K-Means NSA: Threshold=2.5, Detektör Sayısı=1000 ===
Accuracy: 0.9562
Precision: 0.9928
Recall: 0.9132
F1 Score: 0.9513
```


K-Means NSA – PCA
Threshold=2.5, Detektör=3000
Normal
Gerçek Anomali
Tespit Edilen Anomali
PCA Bileşeni 2
PCA Bileşeni 1
8
6
4
2
0
−2
−4
−2
0
2
4

```
=== K-Means NSA: Threshold=2.5, Detektör Sayısı=3000 ===
Accuracy: 0.9508
Precision: 0.9947
Recall: 0.8998
F1 Score: 0.9449
```

- **Threshold**
- Bir örneğin anomali (saldırı) olup olmadığını belirlemek için kullanılan mesafe eşiğidir. Küçük threshold → sıkı kontrol, büyük threshold → daha esnek kontrol sağlar.
- **Accuracy**
- Doğru tahmin edilen örneklerin tüm örneklere oranıdır. Genel başarıyı gösterir.
- **Precision**
- Tespit edilen anomalilerin ne kadarının gerçekten anomali olduğunu gösterir. Yanlış alarm oranı düşükse yüksektir.
- **Recall**
- Gerçek anomalilerin ne kadarının doğru tespit edildiğini gösterir. Düşükse bazı saldırılar gözden kaçıyor demektir.
- **F1 Score**
- Precision ve Recall'un dengeli bir ortalamasıdır. Saldırı tespiti kalitesini genel olarak özetler.

- **Az Detektör (örn. 1000)**
- - Az çeşitlilikte örnek alanı kapsar.
  - Daha az anomaliyi tespit edebilir → **Recall düşebilir**.
  - Hızlı çalışır, işlem yükü azdır.
- **Fazla Detektör (örn. 3000)**
- - Normal davranış alanını daha iyi kapsar.
  - Daha fazla anomali tespit edebilir → **Recall artabilir**.
  - Ancak fazla detektör yanlış alarmları da artırabilir → **Precision düşebilir**.
  - İşlem süresi ve bellek kullanımı artar.
- **Düşük Threshold (örn. 2.5)**
- - Sadece çok uzak örnekleri anomali sayar.
  - Yanlış alarmlar (false positive) azalır → **Precision yüksek**.
  - Ama bazı saldırılar gözden kaçabilir → **Recall düşük**.
- **Yüksek Threshold (örn. 3.0)**
- - Daha fazla örnek anomali olarak sayılır.
  - Saldırıları kaçırma ihtimali azalır → **Recall artar**.
  - Ancak yanlış alarmlar artabilir → **Precision düşebilir**

📌 Getirilebilecek Yenilikler

- 🔄 **Threshold ve detektör sayısının otomatik optimizasyonu** (Grid Search)
- 🔍 **Farklı algoritmalarla karşılaştırma** (Isolation Forest, Autoencoder, One-Class SVM)
- 📊 **ROC AUC ve Confusion Matrix ile detaylı analiz**
- 🌐 **Web arayüzü ile canlı kullanım** (Streamlit, Flask)
- ⚖️ **Veri dengesizliği için SMOTE gibi dengeleme yöntemleri**
- 💾 **Modelin kaydedilip yüklenmesi** (joblib, pickle)
- 🧪 **Farklı veri setleriyle test** (UNSW-NB15, CICIDS2017)
- 📈 **Görselleştirme için t-SNE veya UMAP kullanımı**

📌 Sonuç

- Bu çalışmada, NSL-KDD veri seti kullanılarak negatif seçim algoritmasına (NSA) dayalı iki farklı yaklaşım olan **K-Means NSA** ve **Rastgele NSA** yöntemleri ile anomali tespiti gerçekleştirilmiştir. Özellikle ağ trafiğinde saldırıların otomatik tespiti hedeflenmiştir. Farklı threshold ve detektör sayılarıyla yapılan deneyler sonucunda, parametre seçimlerinin başarı oranlarını doğrudan etkilediği gözlemlenmiştir.
- K-Means NSA yöntemi, normal trafiği daha etkili temsil eden merkezlerle daha yüksek doğruluk ve F1 skorları sağlamış; Rastgele NSA ise daha düşük işlem maliyetiyle esnek bir tespit sistemi sunmuştur. Her iki yöntemde de threshold değeri arttıkça saldırı tespit oranı (recall) artmakta, ancak yanlış pozitif oranı da yükselmektedir.
- Genel olarak, bağışıklık sisteminden esinlenen bu yaklaşımların ağ güvenliği alanında etkili, ölçeklenebilir ve açıklanabilir çözümler sunduğu sonucuna varılmıştır. Geliştirmeye açık yönleri ile birlikte, gerçek zamanlı sistemlere entegre edilebilecek potansiyele sahiptir.

KAYNAKÇA

- *Dasgupta, D. (1999). Artificial immune systems and their applications. Springer-Verlag.*
- *Forrest, S., Perelson, A. S., Allen, L., & Cherukuri, R. (1994). Self-nonself discrimination in a computer. Proceedings of the IEEE Symposium on Research in Security and Privacy, 202–212. https://doi.org/10.1109/RISP.1994.296580*
- *Gonzalez, F. A., & Dasgupta, D. (2002). Anomaly detection using real-valued negative selection. Genetic Programming and Evolvable Machines, 4(4), 383–403. https://doi.org/10.1023/A:1020553624945*
- *NSL-KDD Dataset. University of New Brunswick. https://www.unb.ca/cic/datasets/nsl.html*
- *Lichodzijewski, P., & Heywood, M. I. (2008). Real-time credit card fraud detection using a hybrid evolutionary algorithm. Proceedings of the 10th Annual Conference on Genetic and Evolutionary Computation (GECCO), 149–156.*