Hitit Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği

AĞ Trafiği Yönetiminde Yapay Zeka

214210056 Eray ELAGÖZ

Dr. Öğr. Üyesi **Yusuf Alaca**

Çorum

2025 OCAK

İçindekiler

Özet

Bu çalışma, ağ trafiği yönetiminde yapay zeka (YZ) kullanımının faydalarını ve uygulanabilirliğini kapsamlı bir şekilde ele almaktadır. Günümüzde dijital dönüşüm, ağ altyapılarında hızlı bir şekilde artan veri trafiği hacmini beraberinde getirmektedir. Cisco'nun öngörülerine göre, 2025 yılına kadar global ağ trafiği her ay 500 eksabaytı aşacaktır. Bu devasa veri hacmi, ağ yöneticilerini daha verimli ve akıllı çözümlere yönlendirmekte, geleneksel yöntemlerin sınırlamalarını belirgin hale getirmektedir. YZ tabanlı sistemler, bu ihtiyaçlara yanıt veren yenilikçi bir yaklaşım sunmaktadır. Ağ trafiği yönetimi, bir ağın performansını optimize etmek, güvenliğini artırmak ve anomalileri tespit etmek için kritik bir disiplindir. Anlık veri akışlarını analiz etmek, güvenlik açıklarını belirlemek ve kaynakları en etkin şekilde kullanmak gibi çok yönlü işlevlere sahiptir. Geleneksel sistemler, genellikle statik kurallara dayalıdır ve yeni tehditleri algılamada sınırlı kalmaktadır. YZ ise büyük veri analitiği, makine öğrenmesi ve derin öğrenme yöntemleriyle bu alanda bir devrim yaratmaktadır. YZ tabanlı sistemler, trafik optimizasyonu ve siber güvenlikte geniş bir yelpazede uygulanabilirlik göstermektedir. Örneğin, bir cihazdan gelen olağandışı veri akışları hızlı bir şekilde tespit edilerek önlemler alınabilir. Aynı zamanda bant genişliği yönetimi ve öncelikli veri akışlarının belirlenmesi gibi süreçlerde de önemli avantajlar sunar. Bu teknolojiler, ağ üzerindeki normal davranışları öğrenir ve bu örüntülerden sapmaları otomatik olarak algılar. Ayrıca, bu çalışmada yer verilen algoritmalar arasında Support Vector Machines (SVM), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) ve Long Short-Term Memory (LSTM) gibi makine öğrenmesi ve derin öğrenme modelleri öne çıkmaktadır. Bu algoritmalar, veri kümelerindeki ilişkileri analiz ederek daha hassas ve güvenilir sonuçlar üretmektedir. Örneğin, RNN zaman serisi analizinde kullanılırken, LSTM uzun süreli bağımlılıkları anlamada önemli bir rol oynar. Bu modellerin hiperparametre optimizasyonuyla daha yüksek doğruluk oranları elde edilmektedir.

Bu çalışma, YZ destekli ağ yönetim sistemlerinin avantajlarını yalnızca teorik düzeyde değil, aynı zamanda gerçek dünya uygulamalarıyla da desteklemektedir. Trafik yoğunluğunun doğru bir şekilde tahmin edilmesi, olası güvenlik tehditlerinin hızlı bir şekilde algılanması ve kaynakların daha etkin bir şekilde yönetilmesi gibi unsurlar, bu sistemlerin işletmelere sağladığı katkıları göstermektedir. Gelecekte, IoT cihazlarının artışı ve ağların daha karmaşık hale gelmesiyle birlikte,

1. Giriş

Dijitalleşmenin hızla artması, bilgi ve iletişim teknolojilerinde büyük bir dönüşümü beraberinde getirmiştir. Bu dönüşüm, ağ altyapılarında yoğun bir veri trafiği oluşmasına neden olmuştur. İnternet kullanıcılarının artışı, IoT cihazlarının yaygınlaşması ve 5G teknolojisinin kullanıma girmesi gibi faktörler, ağ trafiği miktarını daha da artırmaktadır. Cisco'nun tahminlerine göre, 2025 yılına kadar global ağ trafiği her ay 500 eksabaytı aşacaktır. Bu kadar büyük bir veri akışı, ağ altyapılarının verimli bir şekilde yönetilmesini giderek daha karmaşık hale getirmektedir.

Ağ trafiği yönetimi, bu karmaşıklığı kontrol altına almak ve verilerin güvenli, hızlı ve etkili bir şekilde iletilmesini sağlamak için kullanılan yöntem ve teknolojileri kapsar. Ağ performansının artırılması, trafik yoğunluğunun izlenmesi ve anomali tespiti, ağ yönetiminin temel unsurlarıdır. Ancak geleneksel yöntemler, artan veri miktarı ve sürekli değişen tehditlere karşı genellikle yetersiz kalmaktadır. Bu noktada, yapay zeka (YZ) tabanlı çözümler, ağ trafiği yönetiminde yeni bir paradigma oluşturmaktadır.

YZ destekli ağ yönetim sistemleri, büyük veri analitiği, makine öğrenmesi ve derin öğrenme gibi ileri teknolojilerden faydalanır. Bu sistemler, normal ağ davranışlarını öğrenip sapmaları tespit ederek gerçek zamanlı ve proaktif çözümler sunar. Bunun sonucunda, yalnızca ağ performansı optimize edilmekle kalmaz, aynı zamanda siber güvenlik tehditlerine karşı daha etkin bir koruma sağlanır.

Bu çalışma, ağ trafiği yönetimi ve yapay zekanın bu alandaki rolünü detaylı bir şekilde incelemeyi amaçlamaktadır. İlk olarak, ağ trafiği yönetiminin temel kavramları ve geleneksel yöntemlerin sınırlamaları tartışılacaktır. Ardından, yapay zekanın ağ trafiği analizi, anomali tespiti, trafik optimizasyonu ve ağ izleme gibi uygulamalarına odaklanılacaktır. Kullanılan algoritmalar, veri işleme yöntemleri ve gerçek hayat uygulamaları bu bağlamda ele alınacaktır. Ayrıca, YZ tabanlı sistemlerin etik kullanımı ve potansiyel riskleri de değerlendirilecektir.

Son olarak, bu çalışmada geliştirilen yapay zeka tabanlı bir mobil uygulama prototipi üzerinden, modern ağ yönetiminde YZ'nin pratik faydaları ortaya konulacaktır. Bu uygulama, ağ trafiğini izleyerek anormal davranışları tespit etmekte ve kullanıcıyı gerçek zamanlı olarak bilgilendirmektedir. Prototip, siber güvenlik tehditlerine karşı alınabilecek önlemlerin etkinliğini de göstermektedir.

2. Ağ Trafiği Yönetimi

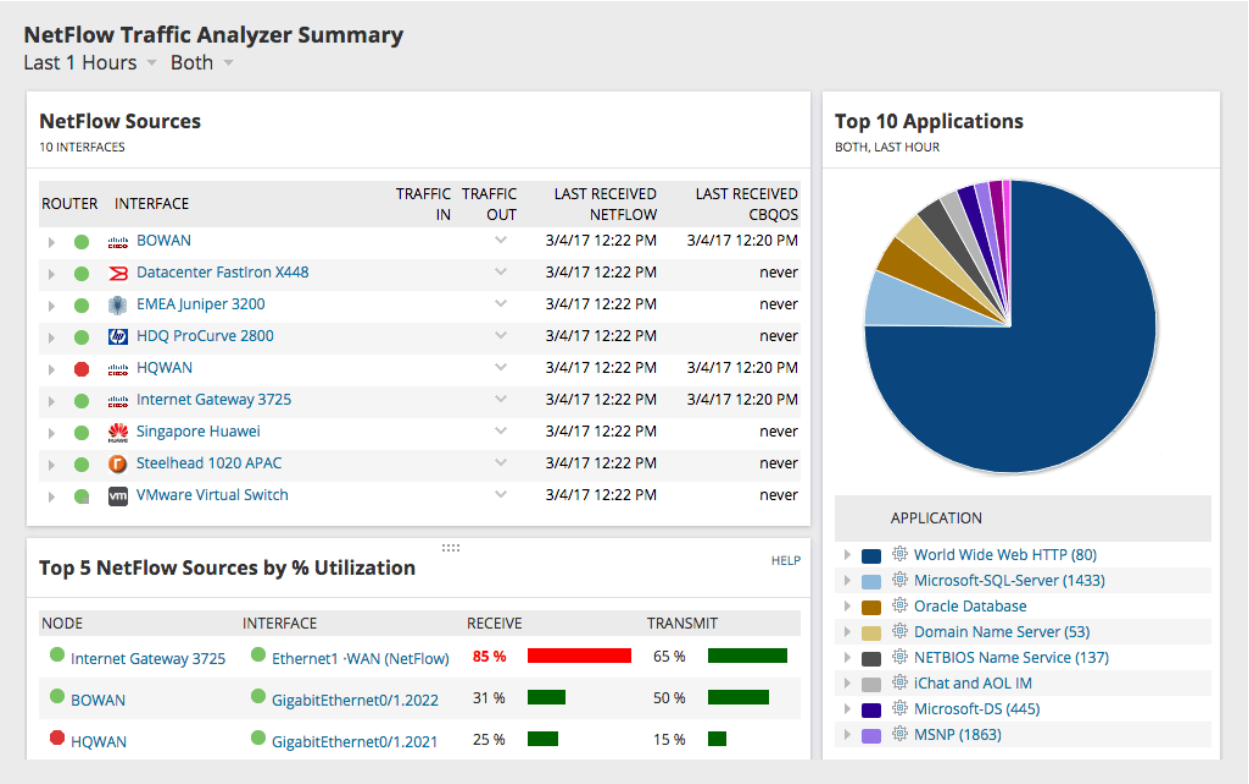
Bu bölümde Ağ Trafiğinin ve Yönetiminin ne olduğu ve bunu neden yaptğıımıza dair bilgileri içerir.

2.1. Ağ Trafiği Yönetimi Nedir?

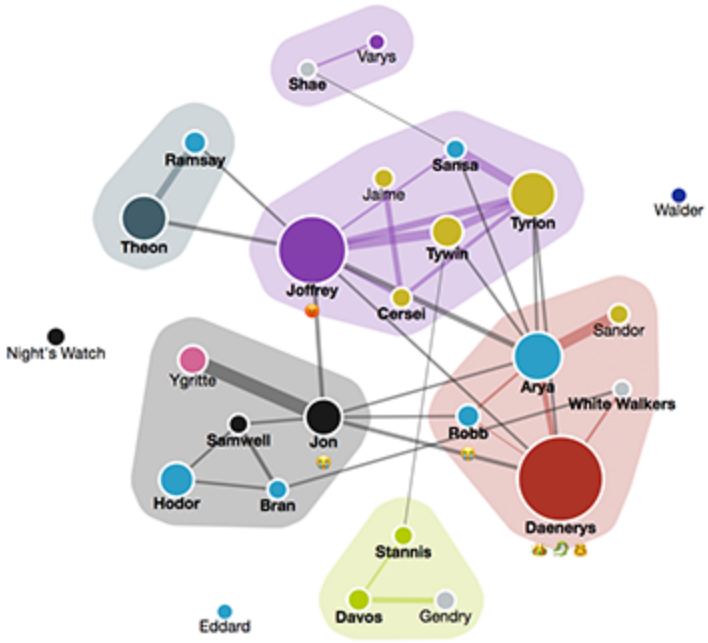
Ağ trafiği yönetimi, bir ağ üzerinde gerçekleşen veri trafiğinin izlenmesi, analiz edilmesi ve gerektiğinde kontrol edilmesi sürecini ifade eder. Bu süreç, ağ performansını artırmak, ağ güvenliğini sağlamak ve ağ kaynaklarının etkin bir şekilde kullanılmasını mümkün kılar.

Ağ trafiği yönetimi, aşağıdaki ana bileşenleri içerir:

1. **Trafik İzleme:** Ağ üzerindeki veri paketlerinin kaynak, hedef, protokol ve içerik gibi bilgilerini toplar. Bu izleme, ağ cihazları (ör. yönlendiriciler ve anahtarlar) üzerinden gerçek zamanlı veya geçmişe dönük olarak yapılabilir.[1]



2. **Veri Analizi:** İzlenen trafik verileri, ağın performansı ve güvenliği açısından analiz edilir. Bu analizler, ağ trafiği yoğunluğu, anomali tespiti ve saldırı algılama gibi konularda kritik bilgiler sağlar.



3. **Önleyici ve Düzeltici Önlemler:** Ağ trafiğinde meydana gelebilecek sorunlar tespit edildiğinde, otomatik veya manuel müdahalelerle bu sorunların çözülmesi sağlanır. Örneğin, bir DDoS saldırısı algılandığında, saldırıya neden olan IP adreslerinin engellenmesi gibi işlemler yapılabilir.

Ağ trafiği yönetiminin önemi, özellikle büyük ölçekli ağ altyapılarında daha da artar. İşletmeler için ağ performansının optimize edilmesi, hizmet kesintilerinin önlenmesi ve verilerin güvenliğinin sağlanması operasyonel sürdürülebilirliğin temel unsurlarındandır.

2.2. Neden Ağ Trafiği Analizi Yapıyoruz?

Ağ trafiği analizi, ağ yönetiminin ayrılmaz bir parçasıdır ve çeşitli amaçlara hizmet eder. Fiyat/Performans analizleri sistemlerin uyumsuzluğu gibi konuların açıklanması, ağ trafiği analizinin neden yapıldığına dair başlıca nedenler detaylı olarak açıklanacaktır.

2.2.1. Performans ve Kaynak Kullanımı

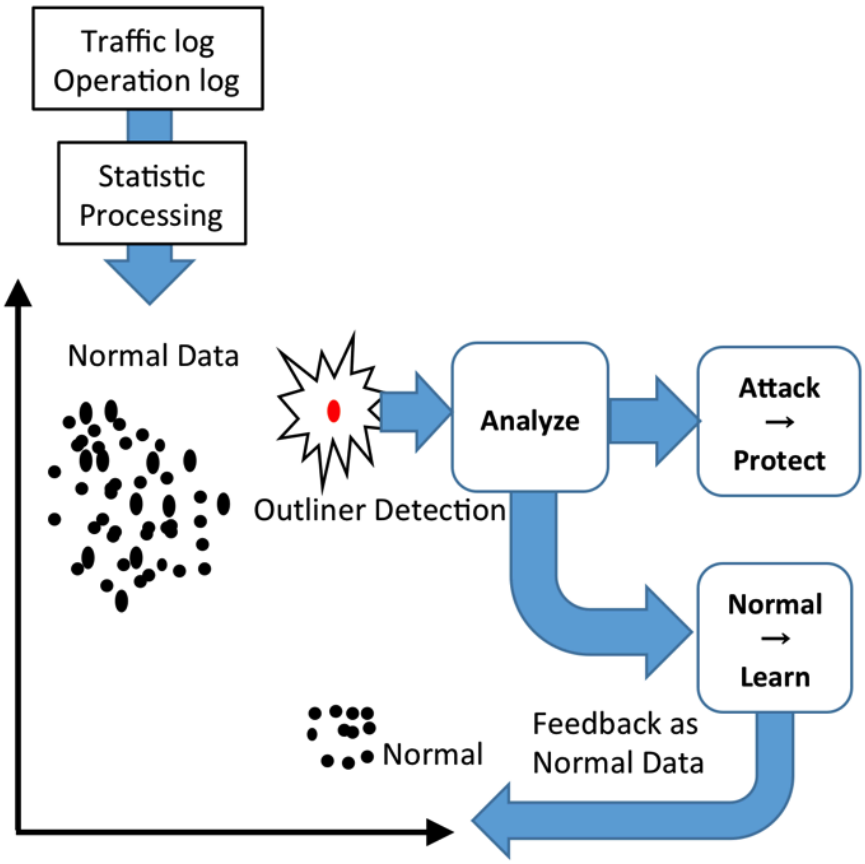
1. **Bant Genişliği Yönetimi:** Ağ trafiği analizi, ağda mevcut bant genişliğinin nasıl kullanıldığını anlamaya yardımcı olur. Yoğun saatlerde ağın tıkanmasını önlemek ve hizmet kalitesini artırmak için belirli uygulamalara veya cihazlara öncelik verilebilir.

2. **Gecikme ve Veri Kaybı Optimizasyonu:** Gecikme süreleri ve veri kaybı oranları analiz edilerek ağ performansı artırılabilir. Örneğin, gerçek zamanlı iletişim gerektiren VoIP ve video konferans gibi uygulamalarda gecikme sürelerinin minimize edilmesi kritik öneme sahiptir.

3. **Maliyet Yönetimi:** Ağ performansını optimize ederek daha az kaynak kullanımıyla daha fazla verimlilik sağlanabilir. Bu da işletmelerin maliyetlerini düşürmesine katkı sağlar.

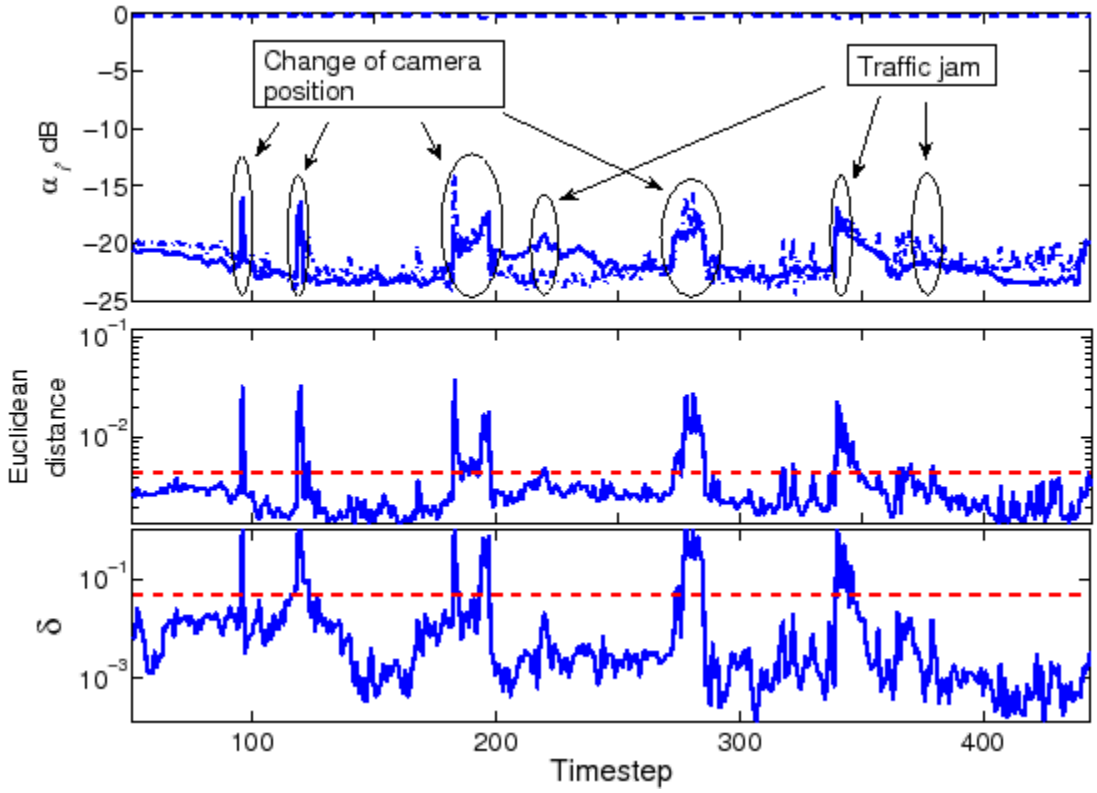
2.2.2. Güvenlik Denetimi

1. **Siber Saldırı Tespiti ve Önleme:** DDoS saldırıları, brute force girişimleri ve kötü amaçlı yazılımlar gibi tehditlerin tespit edilmesi için ağ trafiği analiz edilir. Bu analizler, şüpheli aktiviteleri tespit etmek ve gerektiğinde koruyucu önlemler almak için kullanılır.



2. **Anomali Tespiti:** Ağ trafiğindeki normal davranış desenleri ile anormal durumlar karşılaştırılarak, olası tehditler önceden tespit edilebilir. Örneğin, normalden yüksek

miktarda veri gönderimi yapan bir cihaz, bir saldırganın kontrolünde olabilir.



3. **Güvenlik Politikalarının Güçlendirilmesi:** Trafik analizi, mevcut güvenlik politikalarının etkinliğini değerlendirmek ve gerekli güncellemeleri yapmak için bir temel sağlar.

2.2.3. Sorun Tespiti

1. **Ağ Tıkanıklıklarının Belirlenmesi:** Trafik analizleri, belirli bir bölgede veya zamanda yoğunlaşan trafiği tespit ederek ağ tıkanıklıklarını önleme imkanı sunar.

2. **Bağlantı Kesintileri:** Ağda meydana gelen kesintilerin nedenlerini analiz ederek hızlı bir şekilde çözüme ulaşılabilir.

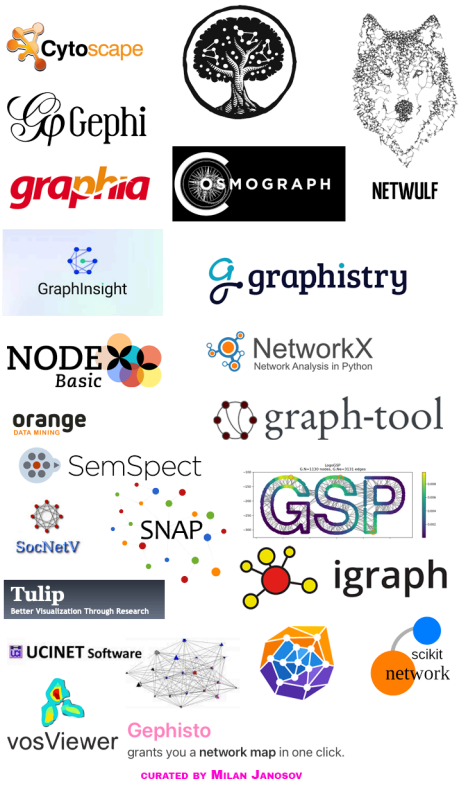
3. **Anormal Trafik Aktiviteleri:** Örneğin, belirli bir IP adresinden gelen yoğun trafik, bir brute force saldırısı veya yanlış yapılandırılmış bir cihazdan kaynaklanıyor olabilir. Trafik analizi, bu durumların tespit edilmesi için kritik öneme sahiptir.

2.2.4. Ek Bileşenler ve Uygulamalar

Ağ trafiği yönetiminde kullanılan araçlar ve yöntemler, ağ izleme, protokol analizi, trafik sınıflandırması ve raporlama gibi işlevleri içerir. Bu işlevler, ağ yöneticilerinin proaktif bir şekilde sorunları çözmesine ve ağın genel sağlığını korumasına olanak tanır.

Örneğin:

1. **Ağ İzleme Araçları:** Wireshark, SolarWinds ve Nagios gibi araçlar, ağdaki trafiği detaylı bir şekilde izlemek ve analiz etmek için yaygın olarak kullanılmaktadır..[2]

2. 

3. **Trafik Sınıflandırması:** Ağ trafiği, kaynak ve hedef bilgileri, protokoller ve içerik türlerine göre sınıflandırılarak daha iyi bir yönetim sağlanır.

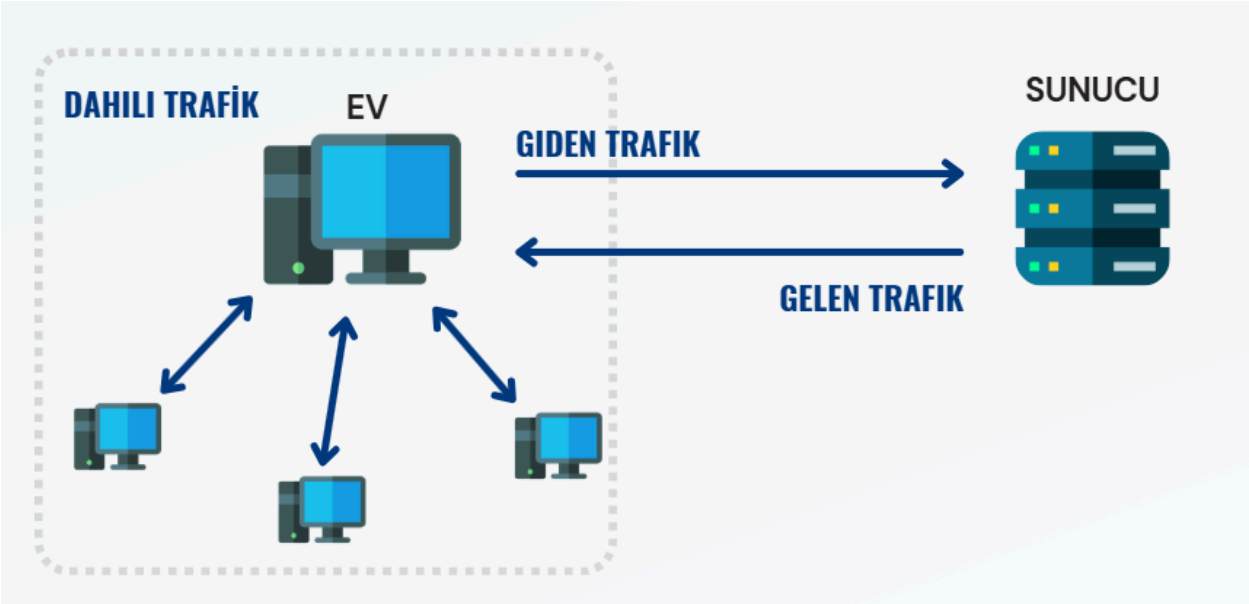
Bu detaylar, ağ trafiği yönetimi ve analizi süreçlerinin anlaşılmasını ve etkin bir şekilde uygulanmasını sağlayarak ağ performansının ve güvenliğinin artırılmasına katkıda bulunur.

3. Ağ Trafiği Türleri

Ağ trafiği, bir ağ üzerindeki veri paketlerinin türüne, yönüne ve protokolüne bağlı olarak çeşitli kategorilere ayrılır. Bu sınıflandırma, ağ yönetiminde ve performans optimizasyonunda kritik bir rol oynar. Aşağıda ağ trafiği türleri detaylı bir şekilde ele alınmaktadır:

3.1. Trafiğin Yönüne Göre

1. **Giden Trafik (Outbound Traffic):**
    a. Tanım: Ağdan dış dünyaya, genellikle internete doğru gerçekleşen veri akışıdır.
    b. Örnekler: Bir kullanıcının bir web sitesine erişim isteği göndermesi, e-posta gönderimi veya bir dosyanın bulut depolama alanına yüklenmesi.
    c. Özellikler: Giden trafik, çoğunlukla kullanıcıların başlattığı işlemleri içerir. Ancak kötü amaçlı yazılımlar veya yetkisiz veri transferleri de bu kategoride yer alabilir ve dikkatle izlenmesi gerekir..[3]
2. **Gelen Trafik (Inbound Traffic):**
    a. Tanım: Dış kaynaklardan ağ içine doğru gerçekleşen veri akışıdır.
    b. Örnekler: Bir web sunucusuna gelen ziyaretçi istekleri, e-posta alımı veya bir cihazın yazılım güncellemeleri için gelen veri akışı.
    c. Özellikler: Gelen trafik, ağın dış tehditlere karşı en savunmasız olduğu kategori olarak dikkat çeker. Bu nedenle, güvenlik duvarları ve saldırı algılama sistemleriyle sıkı bir şekilde izlenmelidir.
3. **Dahili Trafik (Internal Traffic):**
    a. Tanım: Aynı ağ içerisindeki cihazlar arasında gerçekleşen veri akışıdır.
    b. Örnekler: Ofis içi dosya paylaşımı, ağ yazıcılarına gönderilen yazdırma komutları veya veritabanı sorguları.
    c. Özellikler: Dahili trafik, dış tehditlerden daha az etkilenir ancak yanlış yapılandırmalar, iç tehditler veya ağ segmentasyon eksiklikleri bu trafiği savunmasız hale getirebilir.[4]

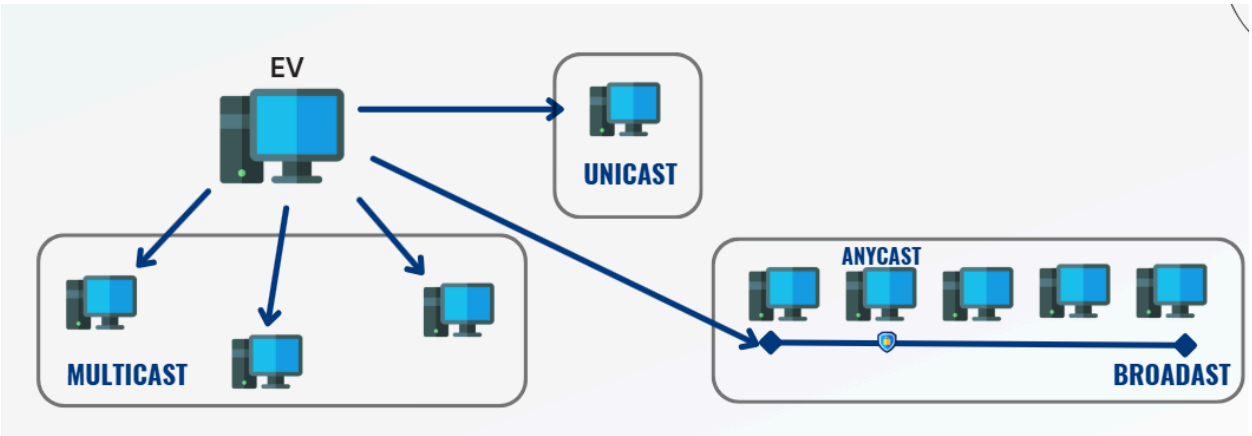


3.2. Trafiğin Hedefine Göre

1. **Unicast Trafik:**
    a. Tanım: Bir kaynaktan yalnızca bir hedefe yönelik veri iletimidir.
    b. Örnekler: Bir bilgisayardan başka bir bilgisayara gönderilen e-posta veya dosya transferi.
    c. Özellikler: Unicast trafik, ağ üzerindeki en yaygın trafik türüdür ve genellikle bire bir iletişim için kullanılır.
2. **Multicast Trafik:**
    a. Tanım: Bir kaynaktan belirli bir grup hedefe yönelik veri iletimidir.
    b. Örnekler: Bir video konferans yayını veya IPTV hizmetleri.
    c. Özellikler: Multicast trafik, birden çok kullanıcıya aynı anda veri göndererek bant genişliğini optimize eder.[5]
3. **Broadcast Trafik:**
    a. Tanım: Bir kaynaktan ağdaki tüm cihazlara yönelik veri iletimidir.
    b. Örnekler: DHCP sunucusunun IP adreslerini dağıtması veya ağ üzerindeki cihazları keşfetmek için yapılan yayılım mesajları.

c. Özellikler: Broadcast trafik, küçük ağlarda kullanışlı olabilir, ancak büyük ağlarda ağ tıkanıklığına neden olabilir.

4. **Anycast Trafik:**
    a. Tanım: Bir kaynaktan en yakın veya en uygun hedefe yönelik veri iletimidir.
    b. Örnekler: DNS sunucularına yapılan istekler.
    c. Özellikler: Anycast trafik, hızlı ve verimli veri iletimi sağlamak için kullanılır ve genellikle küresel hizmetlerin sağlanmasında kritik bir rol oynar.



3.3. Trafiğin Protokolüne Göre

1. **TCP Trafiği (Transmission Control Protocol):**
    a. Tanım: Güvenilir ve bağlantı tabanlı veri iletimi sağlayan bir protokoldür.
    b. Örnekler: Web tarayıcıları (HTTP/HTTPS), e-posta hizmetleri (SMTP, IMAP, POP3).
    c. Özellikler: TCP, veri paketlerinin doğru sırayla ve eksiksiz bir şekilde hedefe ulaşmasını garanti eder. Ancak, bu güvenilirlik ekstra bir yük oluşturabilir, bu nedenle gecikme süreleri diğer protokollere göre daha uzun olabilir.

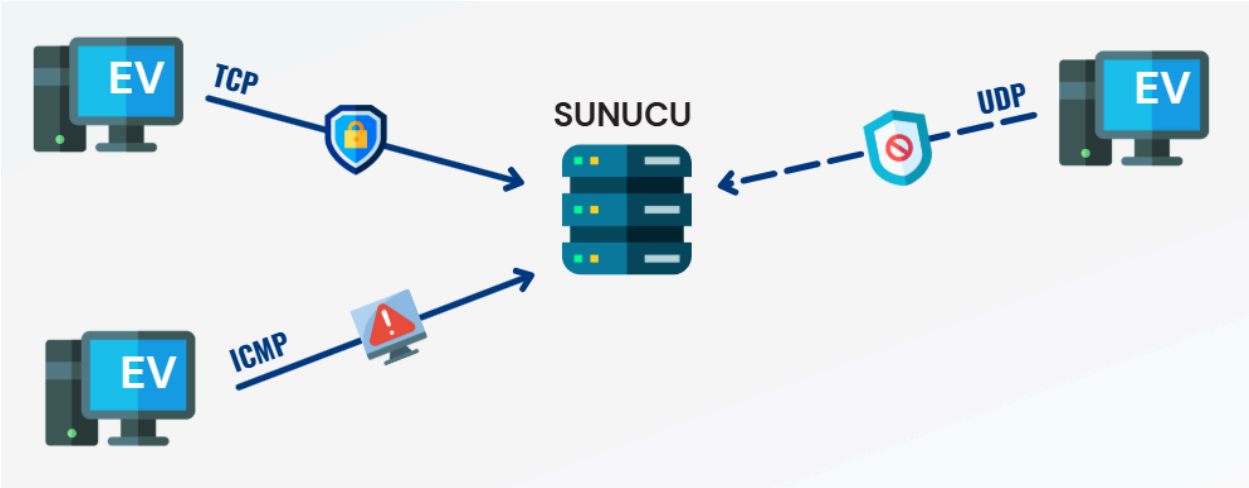
2. **UDP Trafiği (User Datagram Protocol):**
    a. Tanım: Daha hızlı veri iletimi sağlayan ancak güvenilirlik garantisi olmayan bir protokoldür.
    b. Örnekler: Canlı video akışları, online oyunlar, VoIP hizmetleri.

c. Özellikler: UDP, düşük gecikme süreleri gerektiren uygulamalar için idealdir. Ancak veri paketlerinin kaybolma ihtimali vardır.

3. **ICMP Trafiği (Internet Control Message Protocol):**
   a. Tanım: Ağ hatalarını bildirmek ve ağ durumunu tanılama amacıyla kullanılan bir protokoldür.

   b. Örnekler: Ping ve traceroute komutları.

   c. Özellikler: ICMP, genellikle ağ yöneticileri tarafından bağlantı sorunlarını gidermek ve ağ performansını analiz etmek için kullanılır. Ancak, bu protokol bazen siber saldırılar tarafından da istismar edilebilir.[6]



4. Geleneksel Yöntemlerin Yetersizlikleri

Geleneksel ağ trafiği analiz yöntemleri, teknolojinin hızla geliştiği ve tehditlerin sürekli değiştiği bir ortamda giderek yetersiz hale gelmiştir. Bu yöntemler, belirli bir dönem için etkili olsa da, modern ağların karmaşıklığını ve yeni tehdit türlerini karşılayacak esneklikten yoksundur. Aşağıda, bu yetersizliklerin temel nedenleri ve bunların ağ yönetimi üzerindeki etkileri detaylı olarak ele alınmıştır:

4.1. Statik Yapılar

Geleneksel ağ yönetim sistemleri, genellikle kural tabanlı ya da imza tabanlı yapılar üzerine kuruludur. Bu sistemler, yalnızca önceden tanımlanmış tehditleri ve anomalileri algılayabilir:

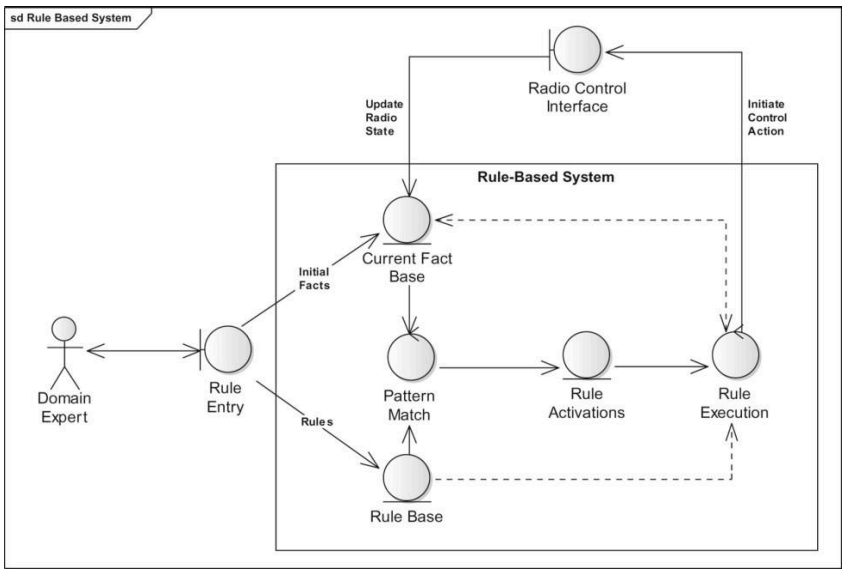
1. **Kural Tabanlı Sistemler:**

   Bu sistemler, belirli olayları tespit etmek için önceden tanımlanmış kurallar ve eşikler kullanır. Örneğin, bir IP adresinden belirli bir süre içinde aşırı miktarda veri gönderildiğinde bir alarm tetiklenir. Ancak bu tür sistemler, değişken ağ dinamiklerine uyum sağlayamaz.

   a. Eksiklikler:

      i. Yeni tehdit türlerini algılayamaz.

      ii. Sürekli olarak manuel güncelleme ve kural setlerinin yeniden tanımlanmasını gerektirir.



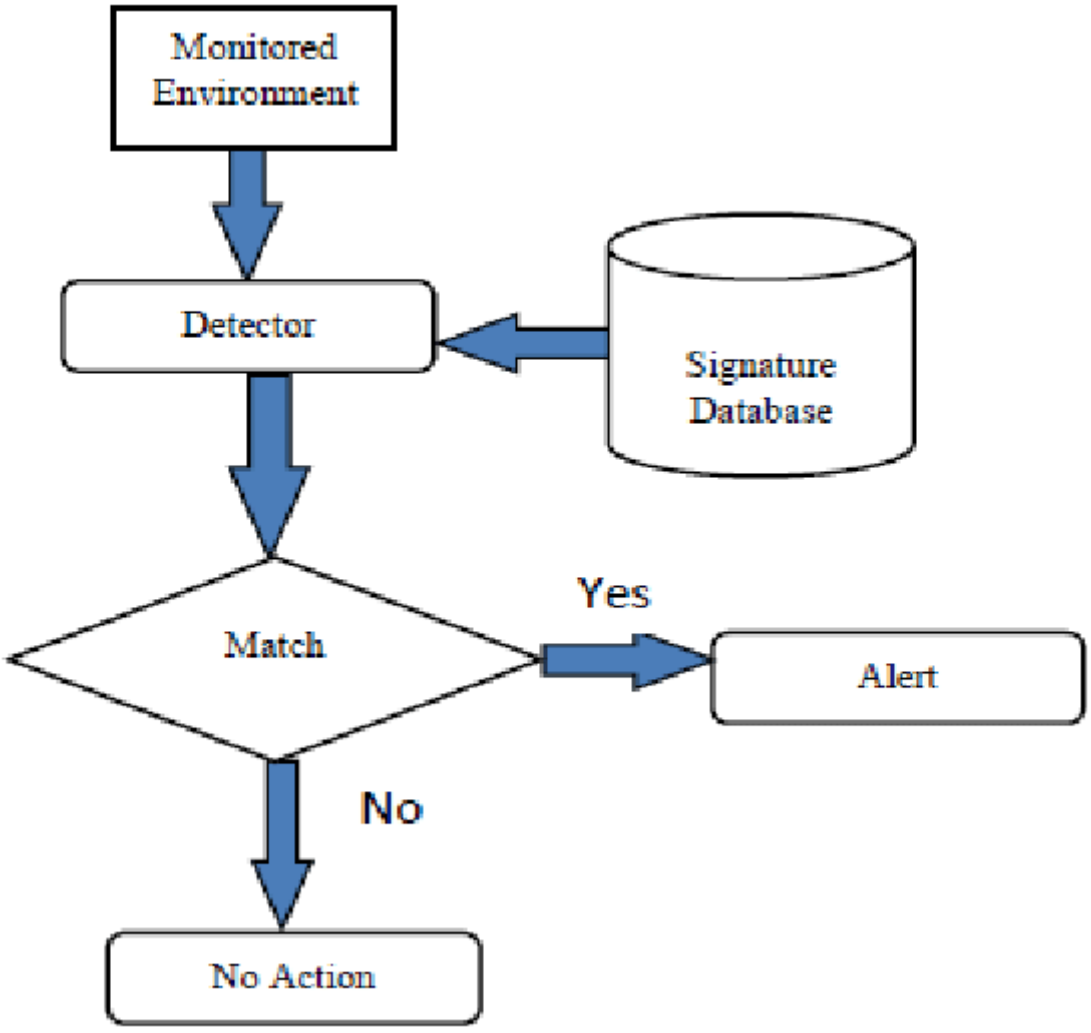
2. **İmza Tabanlı Sistemler:**

   Bu sistemler, bilinen tehditlerin imzalarını (örneğin, bir kötü amaçlı yazılımın belirli bir kod parçası veya bir saldırının protokol davranışı) algılar. Ancak bu yöntem, yalnızca önceden bilinen tehditlere karşı etkilidir.[7]

   a. Eksiklikler:

      i. Zero-day saldırıları gibi daha önce karşılaşılmamış tehditlere karşı savunmasızdır.

      ii. İmza tabanlı sistemlerin sürekli güncellenmesi gerekir, aksi takdirde güncelliğini yitirir.



4.2. Yüksek Maliyet

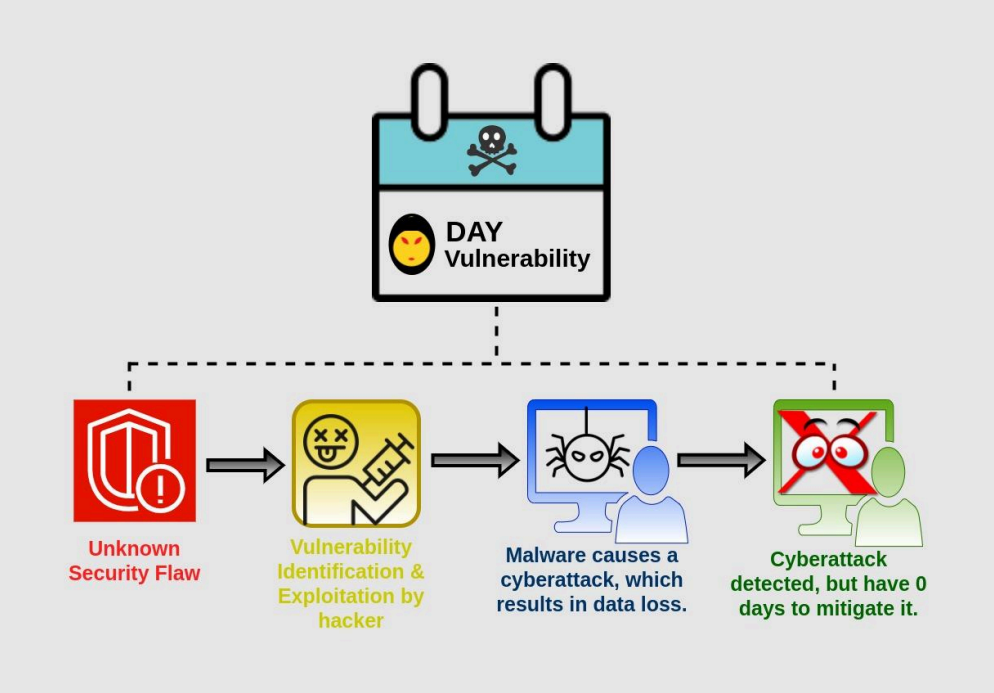
Geleneksel yöntemler, genellikle yüksek operasyonel maliyetlerle ilişkilendirilir. Bu maliyetlerin temel nedenleri:

1. **Manuel İzleme:**
   Geleneksel sistemler, çoğu zaman insan müdahalesine ve manuel analizlere ihtiyaç duyar. Ağ yöneticileri, potansiyel tehditleri belirlemek ve analiz etmek için sürekli olarak ağ trafiğini izlemek zorundadır.
   a. Sonuç: İnsan kaynaklı hata olasılığı artar ve büyük ölçekli ağlarda etkin bir yönetim zorlaşır.
2. **Sürekli Güncelleme:**
   Siber tehditler hızla değiştiği için, geleneksel sistemlerin kural ve imzalarının sürekli olarak güncellenmesi gereklidir. Bu süreç, hem zaman hem de maliyet açısından işletmelere yük getirir.

4.3. Sınırlı Algılama Kapasitesi

Geleneksel ağ yönetim sistemlerinin en belirgin sınırlamalarından biri, bilinmeyen tehditleri algılama konusundaki yetersizliğidir:

1. **Zero-day Saldırıları:**
   Zero-day saldırıları, yazılım veya sistem açıklarını istismar eden ve daha önce keşfedilmemiş saldırı türleridir. Geleneksel yöntemler, bu tür saldırıları algılayacak esnekliğe sahip değildir çünkü bunlar, önceden tanımlı imzalar ya da kurallar tarafından tespit edilemez.



2. **IoT Cihazlarının Etkisi:**

   IoT cihazlarının ağlara eklenmesi, ağ trafiğinin dinamiklerini tamamen değiştirmiştir. Geleneksel sistemler, bu cihazların oluşturduğu büyük miktarda veri trafiğini analiz etmekte ve anomali tespiti yapmakta zorlanmaktadır.

   a. Örnekler:

      i. IoT cihazlarından kaynaklanan DDoS saldırıları.

      ii. IoT cihazlarının güvenlik açıklarından kaynaklanan kötü amaçlı trafik.

4.4. Yeni Tehditlere Karşı Esneklik Eksikliği

Modern ağ tehditleri, yalnızca saldırıları algılamakla kalmayıp, saldırganların davranışlarını öğrenmeyi ve bu davranışlara proaktif bir şekilde yanıt vermeyi gerektirir. Ancak geleneksel yöntemler:[8]

1. **Dinamik Öğrenme Yeteneğine Sahip Değildir:**

   Geleneksel sistemler, makine öğrenmesi veya yapay zeka gibi dinamik öğrenme yeteneklerinden yoksundur. Bu durum, özellikle saldırıların sürekli evrildiği günümüz ağ ortamlarında büyük bir eksikliktir.

2. **Büyük Veri Analitiğine Uygun Değildir:**
   Günümüzde ağlar, büyük miktarda veri üretmektedir. Bu verilerin analiz edilmesi ve anlamlı sonuçlara dönüştürülmesi için güçlü analitik araçlara ihtiyaç vardır. Geleneksel sistemler, bu ölçekte veri işlemek için uygun değildir.

Özet

Geleneksel yöntemler, statik yapıları ve sınırlı algılama kapasiteleri nedeniyle modern ağ tehditlerine karşı yetersiz kalmaktadır. Günümüzün dinamik ve karmaşık ağ ortamlarında, makine öğrenmesi ve yapay zeka tabanlı çözümler gibi daha esnek ve öğrenebilir sistemlere geçiş yapmak gereklidir. Bu tür sistemler, yalnızca bilinen tehditlere değil, aynı zamanda bilinmeyen ve ortaya çıkan tehditlere karşı da etkin bir savunma sağlar. Bu bağlamda, geleneksel yöntemlerin sınırlamaları, modern ağ yönetimi için yapay zeka tabanlı yaklaşımların önemini ortaya koymaktadır.

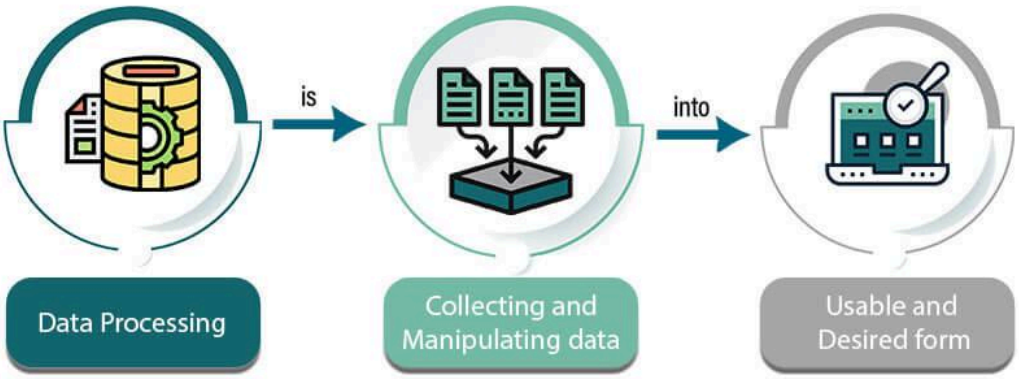
5. Yapay Zeka Destekli Yönetim

Yapay zeka (YZ), ağ trafiği yönetiminde devrim niteliğinde bir değişim yaratmıştır. YZ destekli sistemler, büyük veri kümelerini analiz ederek hem ağ performansını optimize etmekte hem de güvenlik tehditlerini önlemek için etkili çözümler sunmaktadır. Bu bölümde, yapay zeka uygulamalarının detayları ve bu alanda kullanılan algoritmalar ile modeller ele alınacaktır.

5.1. Yapay Zeka Nasıl Uygulanır?

YZ, ağ trafiği yönetimine veri analizi, anomali tespiti ve otomasyon gibi çeşitli şekillerde katkı sağlar. Bu süreçte kullanılan yöntemler şu şekildedir:

1. **Veri Toplama ve Ön İşleme:**
    a. Ağdan gelen veri trafiği sürekli izlenir ve kaydedilir. Bu veri, trafiğin yönü, kaynak ve hedef IP adresleri, zaman damgası, protokoller ve paket boyutları gibi parametreleri içerir.



    b. Toplanan veri, YZ algoritmalarının eğitimi için hazırlanır. Bu süreçte gürültülü veya eksik veriler temizlenir ve uygun formatlara dönüştürülür.

2. **Özellik Seçimi ve Analizi:**
    a. Ağ trafiği analizi için önemli özellikler seçilir. Örneğin, bir cihazın trafik yoğunluğu veya zaman aralıkları belirlenerek modelin öğrenme performansı artırılır.

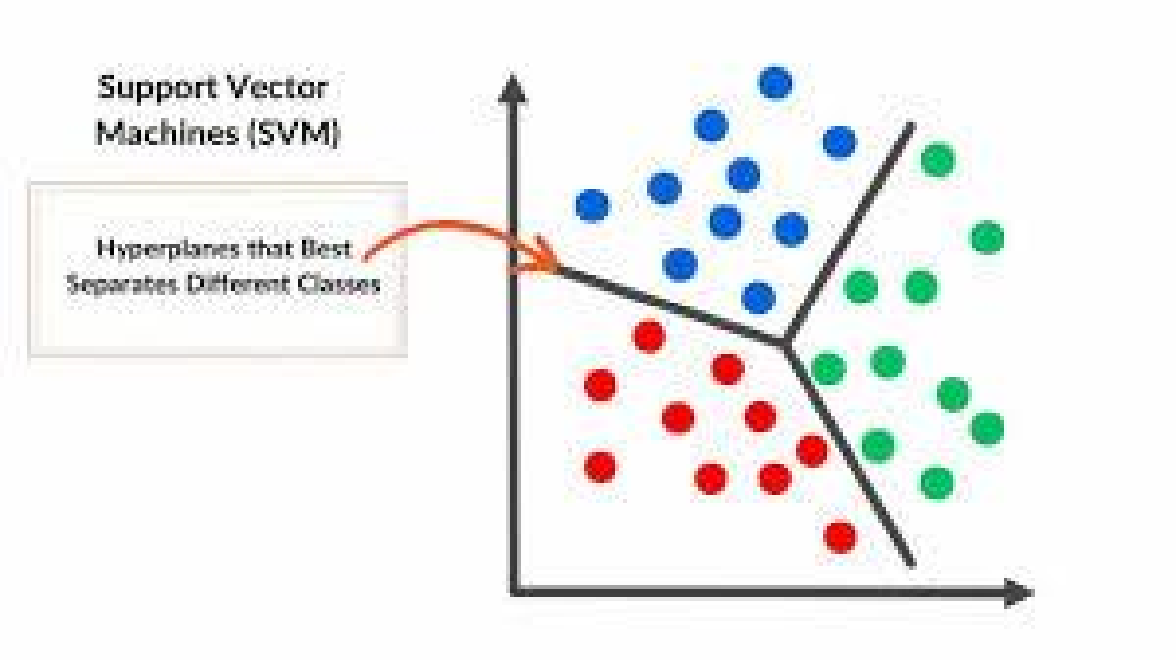
3. **Makine Öğrenmesi ve Derin Öğrenme Yöntemleri:**
    a. Makine öğrenmesi: Örüntüleri öğrenerek geçmiş verilere dayalı tahminler yapar.
    b. Derin öğrenme: Daha karmaşık ve büyük veri kümelerini analiz etmek için çok katmanlı sinir ağlarını kullanır.
4. **Anomali ve Sorun Tespiti:**
    a. YZ, normal trafik davranışlarını öğrenir ve sapmaları tespit eder. Örneğin, bir cihazın trafik davranışında ani bir artış olduğunda, bu durum anomali olarak algılanabilir.
5. **Otomatik Aksiyonlar:**
    a. YZ destekli sistemler, tespit edilen sorunlara otomatik yanıt verebilir. Örneğin, potansiyel bir DDoS saldırısı tespit edildiğinde, saldırı kaynağına ait IP adreslerini otomatik olarak engelleyebilir.

5.2. Kullanılan Algoritmalar ve Modeller

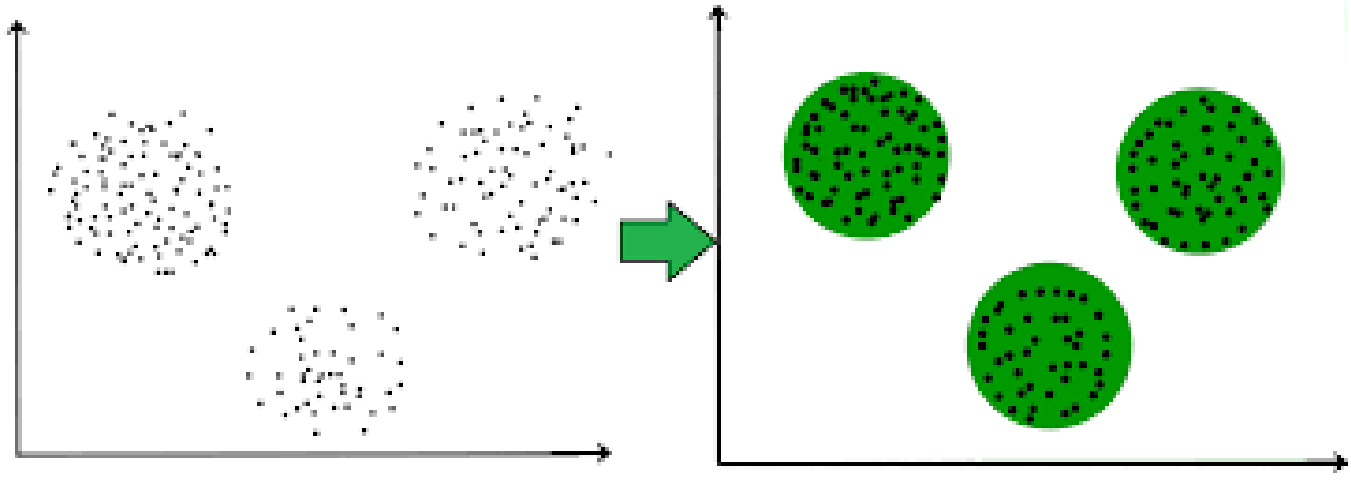
YZ tabanlı ağ yönetiminde kullanılan algoritmalar ve modeller, veri analizi ve sorun çözümünde kritik rol oynar. Bu algoritmalar iki ana kategoriye ayrılır: makine öğrenmesi algoritmaları ve derin öğrenme modelleri.[9]

5.2.1. Makine Öğrenmesi Algoritmaları

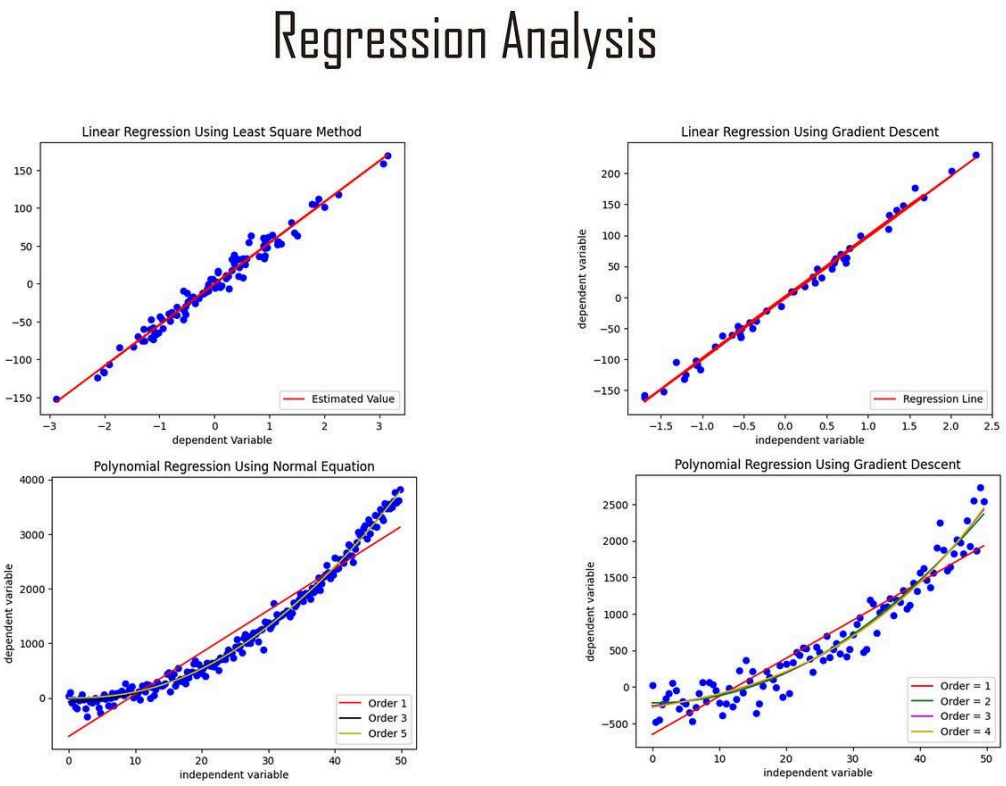
1. **Support Vector Machines (SVM):**
    a. Kullanım Alanı: Anomali tespiti.
    b. Nasıl Çalışır: SVM, veri noktalarını sınıflandırmak için bir hiperdüzlem oluşturur. Anormal trafik örüntüleri, normal davranıştan sapmalar olarak algılanır.
    c. Avantajlar: Yüksek doğruluk ve esneklik. Küçük ve orta ölçekli veri kümeleri için idealdir.



2. **Clustering**:
    a. Kullanım Alanı: Trafik örüntülerinin gruplandırılması ve analizi.
    b. Nasıl Çalışır: K-means veya DBSCAN gibi yöntemler, verileri benzer özelliklere göre gruplandırır. Örneğin, ağ trafiği belirli protokollere veya cihaz türlerine göre sınıflandırılabilir.
    c. Avantajlar: Bilinmeyen trafik davranışlarının keşfedilmesi için uygundur.

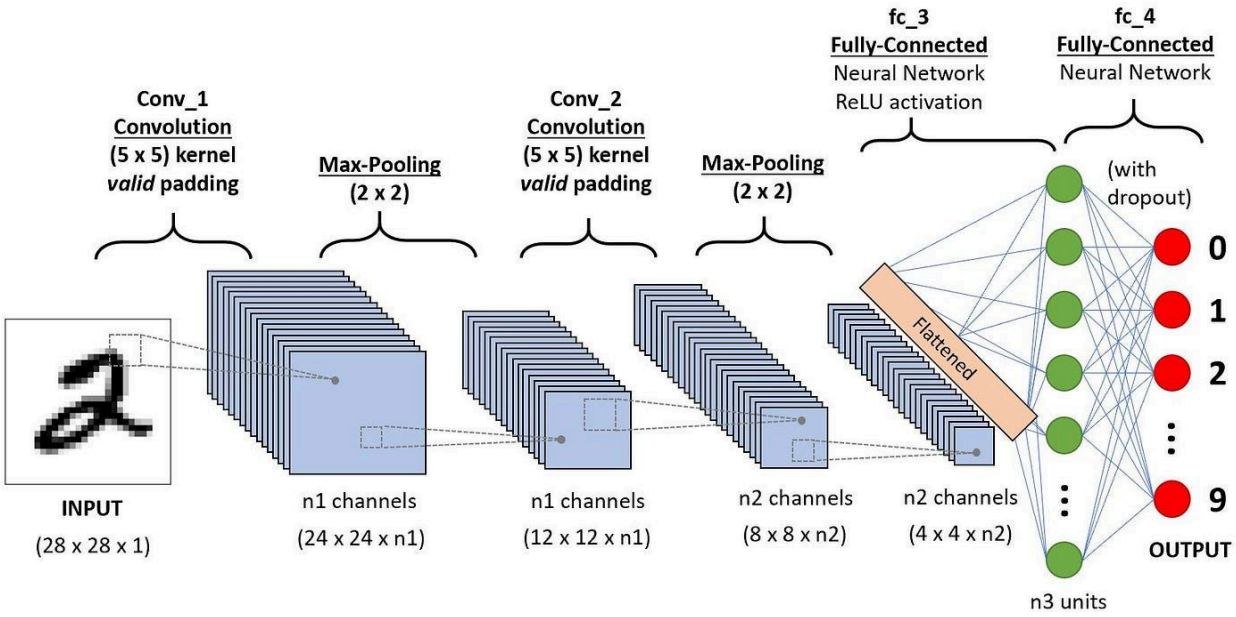


3. **Regression:**
    a. Kullanım Alanı: Trafik yoğunluğu tahmini ve performans analizi.
    b. Nasıl Çalışır: Trafik verileri, zaman serileri kullanılarak analiz edilir ve gelecekteki trafik yükü tahmin edilir.
    c. Avantajlar: Özellikle bant genişliği yönetimi ve önceden planlama için faydalıdır.

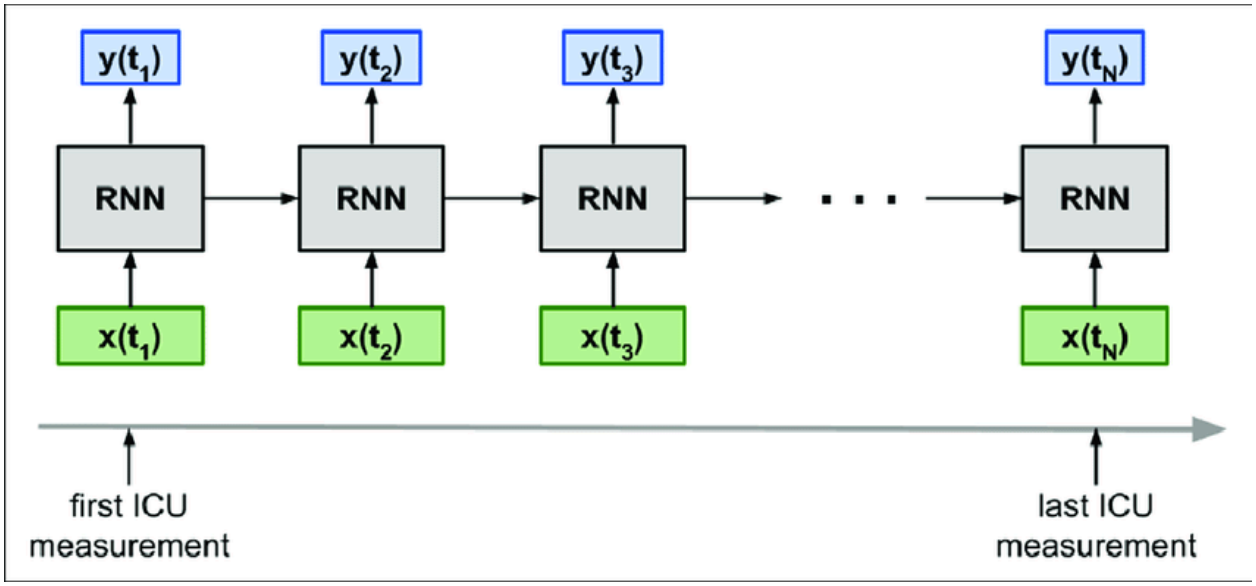


5.2.2. Derin Öğrenme Modelleri

1. **Convolutional Neural Networks (CNN):**
    a. Kullanım Alanı: Görsel trafik analizi ve sınıflandırma.
    b. Nasıl Çalışır: CNN, veri kümelerini iki boyutlu görselleştirmelere dönüştürerek analiz eder. Örneğin, ağ trafiği paketlerinin görselleştirilmesiyle şifreli ve şifresiz trafik ayrımı yapılabilir.
    c. Avantajlar: Görsel tabanlı anomali tespiti ve yüksek doğruluk.



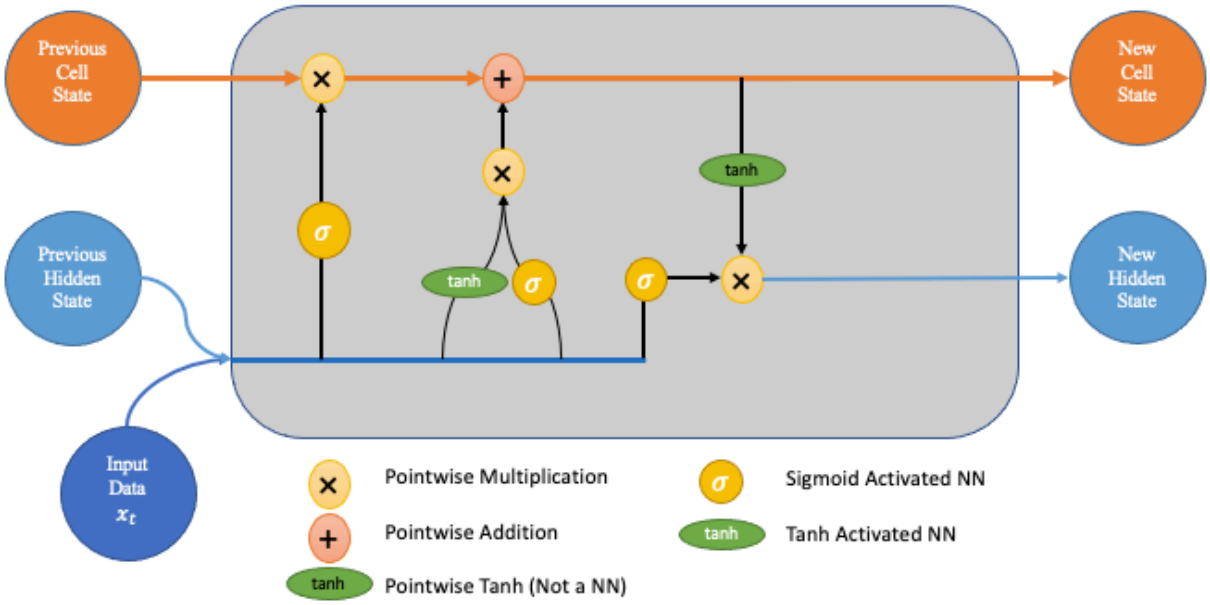
2. **Recurrent Neural Networks (RNN):**
    a. Kullanım Alanı: Zaman serisi analizi.
    b. Nasıl Çalışır: RNN, geçmiş trafik verilerini kullanarak zaman sırasına göre tahminler yapar. Örneğin, bir cihazın trafik yoğunluğunun günlük dalgalanmalarını öğrenir.
    c. Avantajlar: Sıralı veri analizi için uygundur ve zaman bağımlı ilişkileri modelleme yeteneğine sahiptir.



3. **Long Short-Term Memory (LSTM):**
    a. Kullanım Alanı: Uzun süreli veri ilişkilerini anlama ve tahmin yapma.
    b. Nasıl Çalışır: LSTM, RNN'lerin gelişmiş bir versiyonudur ve uzun süreli bağımlılıkları öğrenme konusunda daha etkilidir. Örneğin, bir cihazın trafik yoğunluğunun mevsimsel değişimlerini analiz edebilir. [10]
    c. Avantajlar: Uzun süreli ve karmaşık örüntüleri modellemek için idealdir.

5.3. Yapay Zeka Destekli Sistemlerin Avantajları

1. Hızlı ve Doğru Analiz: Büyük veri kümeleri üzerinde hızlı analiz yaparak gerçek zamanlı çözümler sunar.
2. Dinamik Öğrenme: Trafik davranışlarını sürekli öğrenir ve yeni tehditlere adapte olur.
3. Otomasyon: İnsan müdahalesine gerek kalmadan sorunları tespit eder ve çözüm üretir.
4. Büyük Veri İşleme Yeteneği: Karmaşık ve büyük veri kümelerini işleyerek daha ayrıntılı analizler sunar.



Değerlendirme

Yapay zeka, modern ağ trafiği yönetiminde önemli bir rol oynamaktadır ve bu yöntemlerin uygulanması, ağ performansı ve güvenliğinde önemli iyileştirmeler sağlar. Proaktif ve akıllı ağ yönetiminde, makine öğrenmesi ve derin öğrenme modelleri, işletmelerin ihtiyaçlarını karşılamak için kritik bir altyapı sunar.

6. Veri İşleme ve Modelleme

Veri işleme ve modelleme, yapay zeka tabanlı sistemlerin etkinliğini belirleyen en kritik aşamalardan biridir. Bu süreç, doğru ve güvenilir bir model oluşturmak için ağ trafiği verilerinin işlenmesi, analiz edilmesi ve bir yapay zeka modeline dönüştürülmesini kapsar. Aşağıda bu süreç detaylı bir şekilde ele alınmıştır:

6.1. Veri Toplama ve Ön İşleme

Veri işleme süreci, ağdan gelen trafiğin doğru bir şekilde analiz edilmesi ve model için uygun hale getirilmesi ile başlar.

6.1.1. Veri Toplama

Ağ trafiğinden veri toplama işlemi, modelin temelini oluşturur ve ağ üzerindeki cihazların iletişim davranışlarını anlamak için gerekli olan ham veriyi sağlar.

1. **Toplanan Veri Türleri:**
    a. IP Adresleri: Kaynak ve hedef cihazların belirlenmesi için kullanılır.
    b. Paket Türleri: TCP, UDP veya ICMP gibi protokolleri anlamak için sınıflandırılır.
    c. Zaman Damgaları: Trafik aktivitelerinin zamana göre sıralanmasını sağlar.
    d. Paket Boyutları: Her bir iletişim paketinin büyüklüğü ölçülerek trafik yoğunluğu analiz edilir.
    e. Protokol Bilgileri: Ağ trafiğinin hangi hizmet veya uygulamadan kaynaklandığını anlamak için kullanılır.
2. **Veri Toplama Yöntemleri:**
    a. Ağ İzleme Araçları: Wireshark, SolarWinds veya Nagios gibi araçlar kullanılarak gerçek zamanlı trafik izlenir.
    b. Kayıt Dosyaları: Ağ cihazlarından (örneğin, yönlendiriciler ve sunucular) gelen log dosyaları analiz edilir.

c. Hazır Veri Setleri: KDD Cup veya NSL-KDD gibi yaygın kullanılan veri setleri, model eğitimi için kullanılabilir.

6.1.2. Veri Temizleme

Toplanan veriler, ham haliyle çoğunlukla analiz için uygun değildir ve bu nedenle temizleme sürecinden geçirilir.

1. **Gürültülü Verilerin Ayıklanması:**
   a. Ağ trafiği sırasında toplanan bazı veriler gereksiz veya hatalı olabilir. Örneğin, paket kayıpları veya hatalı zaman damgaları gibi.
   b. Bu tür veriler, modelin performansını olumsuz etkileyebileceğinden temizlenir.
2. **Eksik Verilerin Doldurulması:**
   a. Bazı durumlarda veri setinde eksik bilgiler bulunabilir. Eksik veriler, medyan veya ortalama değerlerle doldurularak veri tutarlılığı sağlanır.
3. **Özellik Çıkarma:**
   a. Verinin anlamlı hale getirilmesi için önemli özellikler seçilir. Örneğin, veri paketlerinin boyutları veya zaman damgaları arasında ilişki kurularak model için kullanılabilir hale getirilir.
4. **Ölçeklendirme:**
   a. Farklı ölçeklerdeki veriler, aynı standartta normalize edilir. Örneğin, paket boyutları ve zaman aralıkları aynı birime indirgenerek analiz sırasında tutarlılık sağlanır.

6.2. Modelleme Süreci

Modelleme süreci, verinin işlenmesinden sonra bir yapay zeka modelinin oluşturulması ve bu modelin performansının optimize edilmesini içerir.

6.2.1. Eğitim ve Test

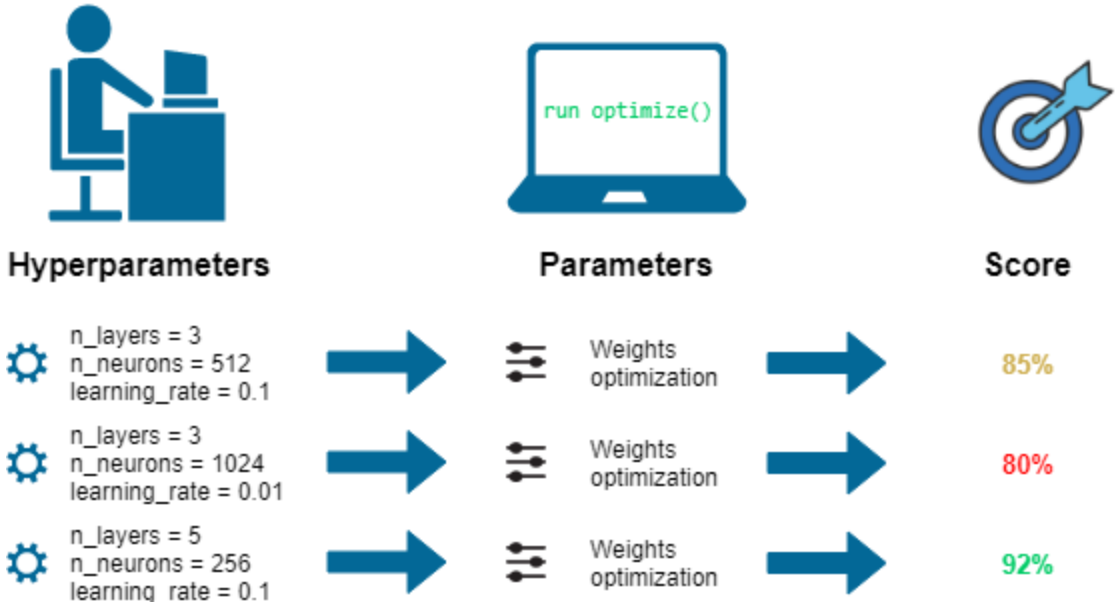
Eğitim ve test işlemleri, modelin doğruluğunu ve genelleştirme yeteneğini değerlendirmek için yapılır.

1. **Veri Bölünmesi:**
    a. Veri seti genellikle eğitim ve test olmak üzere ikiye ayrılır. Yaygın bir bölünme oranı %80 eğitim ve %20 test şeklindedir.
    b. Eğitim seti, modelin öğrenmesi için kullanılırken test seti, modelin yeni verilere ne kadar iyi yanıt verdiğini ölçmek için kullanılır.
2. **Eğitim Süreci:**
    a. Model, eğitim setindeki veriler üzerinde çalışarak veri örüntülerini ve davranışlarını öğrenir.
    b. Örneğin, anormal trafik davranışları ile normal trafik arasında ayrım yapmayı öğrenebilir.
3. **Test Süreci:**
    a. Eğitim sırasında öğrenilen bilgilerin doğruluğu, test setindeki veriler üzerinde kontrol edilir.
    b. Bu süreçte doğruluk, hata oranı ve F1 skoru gibi metrikler kullanılarak modelin performansı değerlendirilir.

6.2.2. Hiperparametre Optimizasyonu

Hiperparametreler, modelin performansını doğrudan etkileyen ayarlardır. Bu parametrelerin doğru şekilde optimize edilmesi, modelin doğruluğunu ve etkinliğini artırır.

1. **Hiperparametreler:**
    a. Öğrenme Oranı: Modelin ne kadar hızlı öğrenmesi gerektiğini belirler.
    b. Epoch Sayısı: Modelin veri üzerinde kaç kez çalışacağını belirtir.
    c. Katman Sayısı ve Nöronlar: Derin öğrenme modellerinde ağın karmaşıklığını belirler.



2. **Optimizasyon Teknikleri:**
    a. Grid Search: Belirli hiperparametre kombinasyonlarını sistematik olarak deneyerek en uygun ayarları bulur.
    b. Random Search: Rastgele hiperparametre kombinasyonları deneyerek daha hızlı bir şekilde optimizasyon sağlar.
    c. Bayes Optimizasyonu: Daha sofistike bir yöntemle olasılık dağılımlarını kullanarak hiperparametrelerin optimize edilmesini sağlar.

6.3. Model Performansının Değerlendirilmesi

Modelleme süreci tamamlandıktan sonra, modelin performansı çeşitli metrikler kullanılarak değerlendirilir:

1. Doğruluk (Accuracy): Modelin doğru tahmin oranını ifade eder.
2. Hassasiyet (Precision): Doğru pozitif tahminlerin toplam pozitif tahminlere oranı.
3. Duyarlılık (Recall): Gerçek pozitiflerin model tarafından tespit edilen pozitiflere oranı.
4. F1 Skoru: Hassasiyet ve duyarlılığın dengeli bir ölçümüdür.

Bu süreçler sonucunda optimize edilmiş ve doğru bir model elde edilerek, ağ trafiği üzerinde etkili bir yönetim ve güvenlik sağlanabilir. Yapay zeka tabanlı sistemler, bu verilerin hızlı ve doğru bir şekilde analiz edilmesine olanak tanır ve ağ yöneticilerinin karşılaşabileceği zorlukları büyük ölçüde azaltır.

7. Uygulama Alanları ve Örnekler

Yapay zeka destekli ağ yönetim sistemleri, hem ticari hem de operasyonel bağlamda geniş bir uygulama yelpazesine sahiptir. Bu sistemler, anomalilerin tespiti, trafik optimizasyonu, performans analizi ve siber güvenlik gibi alanlarda etkili çözümler sunar. Bu bölümde, önde gelen yapay zeka tabanlı çözümler ve bunların kullanım alanları detaylı olarak ele alınmaktadır.

7.1. Cisco Stealthwatch

1. Özellikler:

   Cisco Stealthwatch, ağ trafiğini sürekli olarak izler ve anomalileri tespit etmek için makine öğrenmesi yöntemlerini kullanır.

   a. Ağ içindeki kullanıcı ve cihazların davranışlarını analiz ederek potansiyel tehditleri belirler.

   b. DDoS saldırıları, veri ihlalleri ve şüpheli davranışları tespit edebilir.

2. Uygulama Alanı:

   a. Büyük ölçekli işletmelerde ağ güvenliği sağlamak.

   b. Finansal kurumlarda hassas verilerin korunması.

3. Başarı Örneği:

   a. Cisco Stealthwatch, bir sağlık kuruluşunda fidye yazılımı saldırısını tespit ederek potansiyel veri kaybını önlemiştir.

7.2. Darktrace

1. Özellikler:

   Darktrace, bir yapay zeka platformu olup, ağ trafiğini analiz ederek gerçek zamanlı siber tehdit tespiti yapar.

   a. Özgün bir "Kendi Kendini Öğrenen Yapay Zeka" teknolojisi ile çalışır.

   b. Anomali tespitinde ileri düzey davranışsal analiz yöntemleri kullanır.

c. "Antigena" adını verdiği otonom yanıt sistemiyle tehditlere otomatik olarak müdahale eder.

2. Uygulama Alanı:

    a. Kritik altyapıların korunması (örneğin, enerji şebekeleri ve su dağıtım sistemleri).

    b. Ulusal güvenlik ve savunma ağlarında gerçek zamanlı izleme.

3. Başarı Örneği:

    a. Darktrace, bir havayolu şirketinin müşteri verilerini hedef alan bir saldırıyı erken tespit etmiş ve engellemiştir.

7.3. Aruba NetInsight

1. Özellikler:
   Aruba NetInsight, makine öğrenmesiyle ağ performansını analiz eden ve optimize eden bir sistemdir.

    a. Ağ trafiğini sürekli izler ve performans sorunlarını proaktif olarak tespit eder.

    b. Kullanıcı deneyimini artırmak için öneriler sunar.

2. Uygulama Alanı:

    a. Eğitim kurumlarında öğrenci ve personel ağ bağlantılarının iyileştirilmesi.

    b. Otelcilik sektöründe hızlı ve kesintisiz internet hizmeti sağlanması.

3. Başarı Örneği:

    a. Aruba NetInsight, bir otel zincirinde ağ performansını %35 oranında artırmıştır.

7.4. IBM QRadar

1. Özellikler:
   IBM QRadar, yapay zeka destekli bir güvenlik bilgi ve olay yönetimi (SIEM) platformudur.

a. Tehditleri algılar ve önceliklendirir.

b. Otomatik yanıt mekanizmaları ile tehditlere hızlı müdahale sağlar.

c. Siber saldırıların kaynaklarını analiz eder ve ağ güvenliğini artırır.

2. Uygulama Alanı:

a. Endüstriyel tesislerde siber tehdit yönetimi.

b. Bankacılık sektöründe dolandırıcılık tespiti ve önlenmesi.

3. Başarı Örneği:

a. IBM QRadar, bir telekomünikasyon şirketinde DDoS saldırılarını önleyerek milyonlarca dolarlık zararları engellemiştir.

7.5. Ek Örnekler

1. **Splunk Enterprise Security:**
   a. Özellikler: Makine öğrenmesi ile ağ trafiğini analiz eder ve tehditleri tespit eder.
   b. Uygulama Alanı: Veri merkezlerinde güvenlik tehditlerini tespit etmek ve raporlamak.
   c. Başarı Örneği: Büyük bir perakende zincirinde dolandırıcılık girişimlerini %50 oranında azaltmıştır.
2. **Juniper Networks Mist AI:**
   a. Özellikler: Yapay zeka tabanlı ağ izleme ve optimizasyon platformudur.
   b. Uygulama Alanı: Kurumsal ağlarda kullanıcı deneyimini artırmak ve ağ performansını iyileştirmek.
   c. Başarı Örneği: Bir teknoloji firmasında ağ kesintilerini %70 oranında azaltmıştır.
3. **Palo Alto Networks Cortex XDR:**
   a. Özellikler: Makine öğrenmesiyle uç nokta algılama ve tehdit yanıtı sağlar.

b. Uygulama Alanı: Kapsamlı tehdit yönetimi ve analiz platformu.

c. Başarı Örneği: Küresel bir finans kurumunda kimlik avı saldırılarını başarıyla engellemiştir.

4. **Fortinet FortiAI:**
    a. Özellikler: Derin öğrenme modelleri ile ağ tehditlerini algılar ve önler.

    b. Uygulama Alanı: IoT cihazlarını hedef alan saldırılara karşı koruma sağlamak.

    c. Başarı Örneği: Bir üretim şirketinde IoT tabanlı saldırıları %95 oranında azaltmıştır.

5. **AWS GuardDuty:**
    a. Özellikler: AWS altyapısında çalışan yapay zeka tabanlı bir tehdit algılama hizmetidir.

    b. Uygulama Alanı: Bulut tabanlı hizmetlerin güvenliğini sağlamak.

    c. Başarı Örneği: Bir e-ticaret platformunda veri ihlallerini engellemiştir.

Özet

Yapay zeka destekli çözümler, yalnızca ağ güvenliği ve performansını optimize etmekle kalmaz, aynı zamanda işletmelerin operasyonel verimliliğini artırır. Cisco Stealthwatch, Darktrace, IBM QRadar ve diğer örnekler, bu teknolojilerin ticari ve operasyonel başarısını kanıtlamaktadır. Günümüzde bu tür sistemler, geniş bir yelpazede kurum ve sektör için vazgeçilmez hale gelmiştir. Daha ileri düzey uygulamalar, yapay zekanın ağ yönetiminde sunduğu potansiyeli genişletmeye devam etmektedir.

8. Sonuç ve Değerlendirme

Yapay zeka (YZ), ağ trafiği yönetiminde devrim niteliğinde bir değişim yaratmış, geleneksel yöntemlerin sınırlamalarını aşarak daha etkin ve proaktif çözümler sunmuştur. Modern ağ altyapılarının karmaşıklığı, artan veri hacmi ve sürekli gelişen siber tehditler, YZ tabanlı sistemlerin bu alandaki önemini daha da artırmaktadır. Bu bölümde, YZ'nin ağ trafiği yönetimindeki katkıları ve gelecekteki potansiyeli detaylı olarak değerlendirilmiştir.

8.1. Yapay Zeka Tabanlı Sistemlerin Avantajları

1. **Etkili Güvenlik:**
    a. YZ destekli sistemler, sıfırıncı gün (zero-day) saldırıları, DDoS tehditleri ve kötü amaçlı trafik gibi modern tehditleri algılama ve önlemede oldukça başarılıdır.

    b. Özellikle Darktrace ve IBM QRadar gibi sistemler, davranışsal analiz ve otomatik yanıt mekanizmaları ile proaktif güvenlik sağlar.

2. **Trafik Optimizasyonu:**
    a. YZ, ağ trafiğini analiz ederek bant genişliğini optimize eder, trafiği önceliklere göre yönlendirir ve ağ tıkanıklıklarını önler.

    b. Örneğin, Aruba NetInsight gibi araçlar, kullanıcı deneyimini iyileştirmek için öneriler sunar.

3. **Büyük Veri Analitiği:**
    a. Geleneksel yöntemlerin işleyemediği büyük miktardaki ağ trafiği verileri, YZ tabanlı sistemlerle kolayca analiz edilebilir.

    b. Büyük veri kümelerindeki karmaşık ilişkiler, makine öğrenmesi ve derin öğrenme algoritmaları ile anlamlandırılır.

4. **Otomasyon ve Hız:**
    a. YZ tabanlı sistemler, anomali tespiti ve tehdit önleme gibi işlemleri insan müdahalesine gerek kalmadan hızlı bir şekilde gerçekleştirir.

    b. Örneğin, Cisco Stealthwatch, ağda anormallik tespit edildiğinde otomatik aksiyonlar alır.

8.2. Geleneksel Yöntemlere Göre Üstünlükler

Geleneksel yöntemler genellikle statik kurallara dayanır ve yeni tehditlere karşı esnek değildir. Buna karşın, YZ tabanlı sistemler:

1. **Dinamik Öğrenme Yeteneğine Sahiptir:** Trafik davranışlarını sürekli öğrenir ve yeni tehditlere uyum sağlar.
2. **Gerçek Zamanlı Çözümler Sunar:** Anomali tespitinde ve tehditlere karşı hızlı yanıt vermede üstündür.
3. **Daha Az İnsan Kaynağına İhtiyaç Duyar:** Manuel izleme ve güncelleme gerektirmediği için operasyonel maliyetleri düşürür.

8.3. Gelecekteki Uygulamalar ve Yaygınlık

Yapay zeka tabanlı ağ yönetim sistemlerinin önemi, teknolojinin hızla gelişmesiyle artmaktadır. Gelecekte bu sistemlerin daha yaygın bir şekilde kullanılacağı öngörülmektedir.

1. **5G ve IoT'nin Etkisi:**
    a. IoT cihazlarının yaygınlaşması ve 5G ağlarının devreye girmesiyle birlikte, ağ trafiği yönetimi daha karmaşık bir hal alacaktır.
    b. YZ tabanlı sistemler, bu karmaşıklığı yönetmek ve güvenlik tehditlerini en aza indirmek için kritik bir rol oynayacaktır.
2. **Tam Otomasyon:**
    a. Gelecekte YZ tabanlı sistemler, tam otomasyon sağlayarak insan müdahalesini minimuma indirebilir.
    b. Örneğin, otonom ağ yönetim sistemleri, trafiği kendi kendine optimize ederek ağ tıkanıklıklarını tamamen ortadan kaldırabilir.
3. **Bulut ve Hibrit Çözümler:**
    a. Bulut tabanlı yapay zeka sistemleri, ağ güvenliği ve performans yönetiminde daha etkin çözümler sunacaktır.

b. AWS GuardDuty gibi bulut tabanlı araçlar, bulut altyapılarının güvenliğini sağlamada daha fazla kullanılacaktır.

8.4. Kritik Başarı Örnekleri

- **Cisco Stealthwatch:** Bir finansal kurumda gerçekleştirilen veri ihlalini engelleyerek milyonlarca dolar tasarruf sağlamıştır.
- **Darktrace:** Bir havayolu şirketinde şifrelenmiş veri hırsızlığını tespit ederek müşteri bilgilerinin korunmasını sağlamıştır.[11]
- **Aruba NetInsight:** Bir eğitim kurumunda ağ performansını %40 oranında iyileştirmiştir.https://www.arubanetworks.com/techdocs/NetInsight/Content/ArubaFrameStyles/Overview/Overview.htm[12]
- **IBM QRadar:** Bir telekom şirketinde gerçekleşen DDoS saldırılarını tespit ederek hizmet kesintisini önlemiştir.[13]

8.5. Yapay Zeka Tabanlı Sistemlerin Riskleri

YZ tabanlı sistemlerin birçok avantajına rağmen, dikkate alınması gereken bazı riskler de bulunmaktadır:

- **Etik Sorunlar:** Ağ trafiğini sürekli izleyen sistemler, kullanıcı gizliliği konusunda endişelere yol açabilir.[14]
- **Hatalı Pozitif ve Negatifler:** Yanlış anomali tespiti, gereksiz alarm veya ciddi tehditlerin gözden kaçması gibi sorunlara neden olabilir.
- **Model Eğitimi İçin Veri Gereksinimi:** YZ modellerinin doğru çalışabilmesi için büyük ve kaliteli veri setlerine ihtiyaç duyulmaktadır.[15]

8.6. Sonuç

Yapay zeka, ağ trafiği yönetiminde benzersiz bir çözüm sunmaktadır. Bu sistemler, ağ güvenliğini artırmanın yanı sıra, operasyonel verimlilik sağlayarak işletmelere rekabet avantajı kazandırmaktadır. Gelecekte, daha fazla işletme ve organizasyonun bu teknolojileri benimsemesi beklenmektedir. Ayrıca, YZ tabanlı sistemlerin gelişimiyle birlikte, ağ yönetiminde tamamen otonom ve akıllı çözümler ortaya çıkacaktır.

10. KAYNAKÇA

[1]CISCO Annual Internet Report (March 9, 2020), Erişim Adresi: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[2] What is the Outbound Traffic Control (n.d), Erişim Adresi: https://cyberpedia.reasonlabs.com/EN/outbound%20traffic%20control.html

[3]What is Anycast? (n.d) ErişimAdresi: https://www.cloudflare.com/learning/cdn/glossary/anycast-network/

[4]What Is Transmission Control Protocol TCP/IP? (n.d) ErişimAdresi: https://www.fortinet.com/resources/cyberglossary/tcp-ip#:~:text=What%20does%20TCP%20mean%3F,data%20in%20digital%20network%20communications.

[5] Internet Control Message Protocol (n.d) ErişimAdresi: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

[6]UDP (User Datagram Protocol) Nedir? (n.d) ErişimAdresi: https://turk.net/blog/udp-user-datagram-protocol-nedir/

[7]Ağ Trafiği İzleme Nedir? (n.d) ErişimAdresi: https://www.manageengine.com/tr/netflow/network-traffic-monitor.html

[8] NAD with 88% accuracy (n.d) ErişimAdresi: https://www.kaggle.com/code/indhumalinib/nad-with-88-accuracy

[9] Network Traffic Anomaly Detection with Machine Learning (n.d) ErişimAdresi: https://eyer.ai/blog/network-traffic-anomaly-detection-with-machine-learning/

[10] Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey,(2021) Erişim Adresi https://www.sciencedirect.com/science/article/pii/S0140366421000426?ref=pdf_download&fr=RR-2&rr=8f0f639cbc54b65b

[11] DarkTrace (n.d) ErişimAdresi: https://en.wikipedia.org/wiki/Darktrace

[12]Ariba Insaight: https://www.arubanetworks.com/techdocs/NetInsight/Content/ArubaFrameStyles/Overview/Overview.htm

[13]IBM QRADAR: https://www.ibm.com/products/qradar-siem

[14]AI Riskleri ve Onlemleri: https://builtin.com/artificial-intelligence/risks-of-artificial-intelligence

[15]AI Dataset Requirements: https://postindustria.com/how-much-data-is-required-for-machine-learning/