**Ceyda UYMAZ 200301503**

**Saldırı Tespitinde Makine Öğrenmesi Yöntemlerinin Performans Analizi**

**Giriş:**

İnternete olan ilgi son yıllarda inanılmaz derecede artmış ve artmaya devam etmektedir. İnternete olan ilgi nasıl arttıysa bu ilgiyi suiistimal etmek isteyen kişilerde arttı. Organizasyonların ağ güvenliğini sağlaması çok daha zor hale gelmiştir. Saldırı ve suçlulara karşı ağ güvenliğini sağlamak için birçok farklı güvenlik sistemleri kullanılmaktadır. Saldırı Tespit Sistemleri (STS) ağ güvenliği için kullanılan güvenlik sistemlerden bir tanesidir. Son yıllarda araştırmacılar daha verimli ve etkin bir STS ortaya koymak için birçok çalışma yapmıştır. Yapılan çalışmalarda bencmark veri seti olarak kullanılan veri setlerinin günümüz şartlarını taşımadığı ve değerlendirmelerde doğru sonuçları vermediği görülmüştür. Bu soruna çözüm olması için 2015 yılında yayınlanan UNSW-NB15 veri seti oluşturulmuştur. Bu çalışmanın amacı STS’yi daha verimli ve etkin hale getirmek için kullanılan makine öğrenmesi yöntemlerinin UNSW-NB15 veri seti kullanılarak incelenmesi ve karşılaştırılmasıdır.

**Saldırı Tespit Sistemleri (STS) Nedir:**

STS, hedef sistemin güvenliğinin sürdürülebilmesine olanak sağlamak için bilgisayar sistemlerindeki zararlı yazılımları tanımlayan yazılımsal veya donanımsal sistemlerdir Karşılaşılan saldırılar, bilgi sistemlerinin yetkisiz kullanımına, değiştirilmesine veya tamamen ortadan kaldırılmasına sebep olarak bilgilerin gizlilik, bütünlük ve erişilebilirliğine yönelik tehdit oluşturur. STS bilgisayar güvenliğini sürdürmek için zararlı yazılım aktivitelerini tanımlamayı amaçlayan bir yapıdır (Khraisat et al. 2019). Bilgisayar servislerinin meşru kullanıcıların isteklerine cevap veremeyecek hale getiren aktiviteler saldırı olarak düşünülmektedir. STS’nin hedefi geleneksel güvenlik duvarları tarafından tanımlanamayan ağ trafiğindeki farklı zararlı yazılım türlerinin tanımlanmaktır. Bunun yapılması bilgisayar sistemlerinin gizlilik, bütünlük ve erişilebilirliğini tehlikeye atan olaylar karşısında yüksek koruma sağladığı için hayati öneme sahiptir.

**Kullanılan Yöntemler:**

Bu çalışmasında, denetimli MÖ algoritmaları ele alınmış ve hedefin belirlenmesi için etiketli eğitim verisi kullanılmıştır. Etiketli veri ile eğitim aşaması tamamlandıktan sonra test veri seti ile performans ölçümleri yapılmıştır. Saldırı tespitinin belirlenmesinde kullanılan bu algoritmalar sırayla şunlardır; • K-En Yakın Komşu (KNN) • Rassal Orman (RO) • Adaboost (AB) • Lojistik Regresyon (LR) • Naive Bayes (NB) • Destek Vektör Makineleri (DVM) • Sinir Ağları (SA)

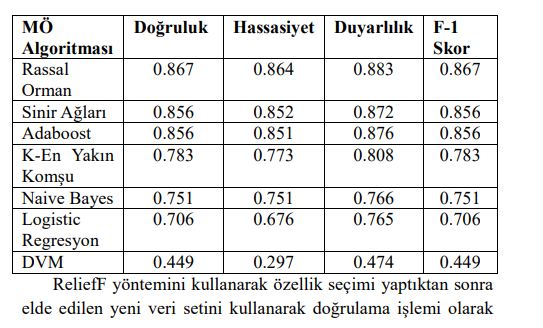
**Kullanılan Veri seti (UNSW-NB15 Veri Seti)**

UNSW-NB15 veri seti IXIA PerfectStorm aracı kullanılarak Avustralya siber güvenlik merkezi laboratuvarlarında hem gerçek modern normal aktivite hem de yapay günümüz şartlarına uygun ağ trafiği saldırı hareketlerini içeren hibrit bir model oluşturulmuştur. UNSW-NB15 veri seti toplam 49 özellik ve 1 hedef değere sahiptir. Çalışmada kullandığımız ve UNSW-NB15 veri setinden oluşturulan alt veri setinden 7 özellik çıkarılmıştır. Çıkarılan özellikler MÖ algoritmalarının kullanabileceği verileri içermediği için çıkartılmıştır. Çıkarılan özelliklerden sonra özellik sayısı 42’ye düşmüştür. Literatürde puanlama yöntemi (scoring method) olarak bilinen ReliefF yöntemi kullanılarak orijinal veri setimizde 42 olan özellik sayısını azaltarak 29’a indilmiştir.

**Uygulama Aracı(Orange) :**Orange, Python ile yazılmış açık kaynak MÖ ve veri madenciliği aracıdır. Veriyi analiz edebilmek ve görselleştirmek için baştan sona görsel programlamaya sahiptir.

Yapılan çalışmada özellik seçimi yapmaksızın orijinal veri ile kullanılan MÖ yöntemleriyle beş farklı kategoride performans değerlendirilmesi yapılmıştır. Özellik seçimi olmaksızın, eğitim veri seti ve test veri seti ayrı olarak kullanılmıştır.

ReliefF yöntemini kullanarak özellik seçimi yaptıktan sonra elde edilen yeni veri setini kullanarak doğrulama işlemi olarak adlandırılan eğitim veri seti ve test veri setinin ayrı ayrı kullanılması sonucunda MÖ yöntemlerinin performanslarının sonuçları Tablo 3‘de verilmiştir.

tablo içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Sonuç:**

**tablo içeren bir resim

Açıklama otomatik olarak oluşturuldu** tablo içeren bir resim

Açıklama otomatik olarak oluşturuldutablo içeren bir resim

Açıklama otomatik olarak oluşturuldu

Olamantanmi ve ark. (Mebawondu et al. 2020) yapmış oldukları çalışmada UNSW-NB15 veri setini kullanmışlardır. Özellik seçimi yaparak MÖ algoritmalarından “sinir ağları” algoritmasını uygulamışlardır. Elde ettikleri sonuçlar ve bu çalışmada elde edilen sonuçlar Tablo 4’de verilmiştir. G.Kocher ve G.Kumar (Kocher and Kumar 2020) 2020 yılında yapmış oldukları çalışmada UNSW-NB veri setini kullanarak MÖ algoritmalarının sınıflandırma performanslarını analiz etmişlerdir. Test veri setini oluştururken eğitim veri seti içerisinden belli oranda test veri seti oluşturulmuştur. Bağımsız bir test veri setleri bulunmamaktadır. Önerdiğimiz yöntemde ise test veri seti ve eğitim veri seti birbirlerinden bağımsız halde kullanılmıştır. Bu çalışmayı önerdiğimiz yöntem ile karşılaştırmanın sağlıklı yapılabilmesi için %20 oranında test işleminin yapılabilmesi gerekmektedir. Karşılaştırılan çalışmada herhangi bir özellik mühendisliği yapılmamış ve literatür kısmında belirttiğimiz gibi özellik sayısı orijinal veri setinde 49 iken 42’ye düşürülmüş ve uygulama yapılmıştır. Elde edilen sonuçlar ve önerdiğimiz yöntem ile elde edilen sonuçlar Tablo 5’de sunulmuştur. G. Kocher ve ark. ve önerdiğimiz çalışmanın MÖ yöntemlerinin performans analizleri Tablo 5’de verilmiştir. Liu Zhiqiang ve ark. (Zhiqiang et al. 2019) yapmış oldukları çalışmada UNSW-NB15 ver setini kullanmışlardır. Yaptıkları çalışmada yeni bir Ağ STS modellemişlerdir.

**Sonuçların Değerlendirilmesi:**

Elde edilen sonuçlar göre en yüksek doğruluk oranına “Rassal Orman” algoritması olmuştur. Veri setinde bulunan 42 özellikten reliefF puanlama yöntemi kullanılarak 42 olan özellik sayısı 29’a indirgenmiş ve MÖ yöntemlerinin performasları tekrar analiz edilmiştir. Elde edilen sonuçlara göre özellik sayısının azalması elde edilen performans değerlerinde artışa sebep olmuştur. Özellik seçimi yaptıktan sonra da en yüksek doğruluk oranına sahip MÖ yöntemi “Sinir Ağları” olduğu görülmüştür. Bu çalışma literatür ile karşılaştırıldığında daha iyi sonuçlar elde ettiği görülmektedir. Bu durumun başlıca sebebi özellik seçimi yaparken kullanılan reliefF yönteminin kullanılmasıdır. Literatürde de elde ettiğimiz bilgilere dayanarak özellikle Nİ cihazlarının heterojen bir yapıdan oluşması ve internet ağındaki kullanımının yoğunlaşması, güvenliği sağlamakta kullanılan MÖ algoritmalarının tek başlarına gösterdikleri performanslarının Topluluk Öğrenimi (TÖ) yöntemlerine nazaran daha düşük olduğudur. İnternet gibi artık heterojen bir yapıya doğru giden ağ sistemlerinde saldırıların tespitinde TÖ yöntemlerinin performans analiz sonuçlarının daha yüksek çıkmasının nedeni karşılaşılan her bir saldırı tipinin farklı MÖ algoritmalarının daha iyi tespit edilebildiğidir.

<https://dergipark.org.tr/en/pub/ejosat/issue/67030/1045551>