

**Fenerbahçe Üniversitesi**

COMP435 - Makine Öğrenmesi

Ödev 2: Saldırı Tespit Sistemlerine Makine Öğrenme Etkisi

Bedirhan İLERİ - 210301501

Günümüzde teknolojinin artmasıyla kötü niyetli siber saldırılar da oldukça artmıştır. Bunun sonucunda insanlar maddi manevi zararlara uğramışlardır. Bu zorbalığı engellemek için çeşitli anti virüs programları veya güvenlik duvarları kullanılmaktadır. Ancak bu her zaman istenilen sonucu elde etmemektedir. Bu makaledeki problem kaynağı budur ve bunu çözmek için makine öğrenmesi tekniklerini, bilinen saldırı çeşitlerini ve sunucu tabanlı saldırı yöntemlerinin verilerini kullanarak saldırı tespit sistemi eğitmek amaçlanmıştır. Bu doğrultuda CesarFTP, WebDAV, Icecast, Tomcat, OS SMB, OS Print Spool, PMWiki, Wireless Karma, PDF N, Backdoored Executable, Browser Attack, Infectious Media saldırı verileri birleştirilerek veri seti oluşturulmuştur.

Bilgi sistemleri ve ağlar elektronik saldırılara maruz kalabilirler. Bilgi güvenliğini ihlal etme girişimleri her gün, internette yaygın olarak bulunan güvenlik açığı değerlendirme araçlarının yanı sıra ticari olarak da kullanılabilen bu araçların kullanılabilirliği ile birlikte artmaktadır. SubSeven, Nmap, L0ftCrack, BackOrifce gibi araçların tümü sistemleri taramak, tanımlamak, araştırmak ve delmek için kullanılabilir. Ağları korumak için güvenlik duvarları ve çeşitli anti virüsler kullanılır. Güvenlik duvarları sizleri dışarıdan gelen saldırılara karşı çok iyi koruyabilir ama eğer sisteminizin içinde bir açık var ise uyarma olasılığı bulunmaz.”Script Kiddie” diye tabir edilen kişiler, interneti sürekli olarak alt ağlar tarafından yapılan taramalar dâhil, bilinen hatalara karşı tarar. Bazı zamanlarda ise, tamamen yasal yollarla rakip bir firma, rekabet avantajı elde etmek için personeller istihdam eder ve oluşturdukları bu ekiple sisteminize sızmaya çalışırlar. Saldırı tespit sistemlerinin önemi bu sebepten ötürü daha iyi anlaşılmaya başlanmıştır. Söz konusu sistemlerin kullanımının bilgi teknolojilerinde %60’dan fazla olduğu 2012 yılında yapılan bir ankette belirtilmiştir. Aktif bir çalışma konusu olmasına ve üzerinde çok sayıda insanın araştırma ve geliştirme yapmasına rağmen, bu tarz saldırıları etkin bir şekilde tespit edebilecek, standartları belirlenmiş bir sistem henüz geliştirilememiştir.

Bu çalışmanın amacı, var olan sunucu tabanlı saldırı çeşitleri ve bunların verilerini kullanarak saldırı tespit sistemini eğitmek, bu şekilde sistemi yeni gelebilecek saldırılara karşı korumaya çalışmaktır. Sistemin her an her çeşit saldırıya karşı koyması hem bellek yönetimi hem de güç tüketimi açısından akıllıca olmayacaktır dolayısıyla gelen saldırının doğru ve etkin bir şekilde sınıflandırılması gerekmektedir. Bu fikirden yola çıkılarak sınıflandırma algoritmaları kullanılmıştır. Saldırının doğru tahmininden sonra bu saldırıya yönelik bir savunma sisteminin devreye girmesi, sistemi amacına ulaştıracak ve minimum hasar ile saldırıyı atlatmayı sağlayacaktır.

Bu çalışmada kullanılan veri seti; CesarFTP, WebDAV, Icecast, Tomcat, OS SMB, OS Print Spool, PMWiki, Wireless Karma, PDF N, Backdoored Executable, Browser Attack, Infectious Media saldırı verileri birleştirilerek oluşturulmuştur. Ortaya çıkan bu veri seti ise Destek Vektör Makinesi (DVM) ve Naive Bayes (NB) kullanılarak sınıflandırılmış ve eğitilmiştir.

Öncelikle kullanılacak veri setleri Düşük Varyans Filtresi, Yüksek Korelasyon Filtresi ve Temel Bileşen Analizi yöntemlerine tabi tutulduktan sonra eğitime hazır bir hale getirilmiştir.

**Düşük Varyans Filtresi**: Veri setinde küçük değişiklikler olan veri sütunları çok az bilgi taşır. Böylece, belirli bir eşikten daha düşük varyansa sahip tüm veri sütunları kaldırılır. Dikkatli edilmesi gereken nokta ise varyans aralığına bağlıdır. Bu nedenle, bu tekniği uygulamadan önce normalizasyon uygulanması gereklidir.

**Yüksek Korelasyon Filtresi:** Çok benzer eğilimlere sahip veri sütunlarının da çok benzer bilgiler taşıması olasıdır. Bu durumda, yalnızca biri makine öğrenme modelini beslemek için yeterli olacaktır. Burada nümerik sütunlar arasında ve sırasıyla Pearson’un Ürün Moment Katsayısı ve Pearson chi kare değeri olarak nominal sütunlar arasındaki korelasyon katsayısı hesaplanır. Korelasyon katsayısı eşikten daha yüksek olan sütun çiftleri yalnızca bir taneye düşürülür.

**Temel Bileşen Analizi(TBA):** Bir veri setinin orijinal n koordinatlarını ortogonal olarak asıl bileşenler adı verilen yeni bir n koordinat grubuna dönüştüren istatistiksel bir prosedürdür. Dönüşümün bir sonucu olarak, ilk ana bileşen olası en büyük varyansa sahiptir; müteakip her bileşen, önceki bileşenlerle korelasyon olmayan kısıtlama altında mümkün olan en yüksek varyansa sahiptir. Yalnızca ilk m<n bileşeninin tutulması, veri bilgisinin çoğunu yani verideki değişimi korurken veri boyutsallığını azaltır.

**Destek Vektör Makinesi (DVM):** Destek vektörleri, hiper düzlemine daha yakın olan ve hiper düzlemin konumunu ve yönünü etkileyen veri noktalarıdır. Bu destek vektörlerini kullanarak, sınıflandırıcının marjı maksimize edilir. Verilerin %90'ı eğitim için, geri kalan %10'u test için kullanılmıştır. Python dili, Numpy kitaplığı kullanılarak DVM modeli oluşturulmuştur. epochs = 1 ve alpha = 0.0001 kullanılarak ilerlenmiştir.

**Naif Bayes:** Naif Bayes modeli, eğitim veri setindeki verilerin bir özetinden oluşur. Bu özet daha sonra tahminlerde bulunurken kullanılır. Toplanan eğitim verilerinin özeti, her özniteliğin sınıf değerine göre ortalamasını ve standart sapmasını içerir. Örneğin, iki sınıf değeri ve 7 sayısal özellik varsa, o zaman her bir özellik (7) ve sınıf değeri (2) kombinasyonu için ortalama ve standart bir sapmaya yani 14 özellik özetine ihtiyaç vardır. Bunlar, her bir sınıf değerine ait belirli özellik değerlerinin olasılığını hesaplamak için tahminlerde bulunurken gereklidir. Bu özet verilerin hazırlanması şu alt görevlere ayırabilir: Verileri sınıflara göre ayırma, hesap ile ortalama, standart sapmayı hesaplama, veri kümesini özetleme ve sınıflara göre öznitelikleri özetleme.

Eğitim verilerinden hazırlanan özetler kullanılarak tahminler yapılabilir. Öngörüler yapmak, verilen bir veri örneğinin her sınıfa ait olma olasılığını hesaplamayı ve ardından tahmin olarak en büyük olasılık olan sınıfı seçmeyi içerir. Bu şu şekilde ayrılabilir: Gauss olasılık yoğunluğu fonksiyonun hesaplama, sınıf olasılıklarını hesaplama, tahmin yapma ve doğruluk tahmini hesaplama. Son olarak, test veri setindeki her veri örneği için tahminler yaparak modelin doğruluğu tahmin edilebilir. GetPredictions() bu tahmini yapar ve her test örneği için bir tahmin listesi döndürür. Tahminler, test veri setindeki sınıf değerleri ile karşılaştırılabilir ve bir sınıflandırma doğruluğu, %0 ve %100 arasında bir doğruluk oranı olarak hesaplanabilir. GetAccuracy() bu doğruluk oranını hesaplar.

DVM algoritmasının seçilmesinin sebebi: DVM’nin net bir ayrılma marjı ile gerçekten iyi çalışması, yüksek boyutlu alanlarda etkili olması, boyut sayısının örnek sayısından daha büyük olduğu durumlarda etkili olması, karar işlevinde de bir eğitim noktaları alt kümesi kullanması, bu nedenle de belleği etkin bir şekilde kullanmasıdır. Naif Bayes algoritmasının tercih edilme sebebi ise, destek vektör makinesi ile birlikte kullanıldığında nasıl bir sonuç vereceğini izlemek ve daha iyi bir sınıflandırma yapabiliyor mu onu test etmektir.

**SONUÇ**

Çalışmada oluşturulan veri kümesine ilk olarak Destek Vektör Makinesi algoritması uygulanmış, 6013 tane veri içerisinden 4287 tanesi doğru tahmin edilirken 1726 tanesi yanlış tahmin edilmiştir. Başarı oranı yaklaşık 0.71 olmuştur. Başarı oranını arttırmak için ikinci bir sınıflandırma algoritması kullanılmak istenmiştir. Var olan veri seti boyut azaltma ve temel bileşen analizine tekrar tabi tutulmuştur ve ardından eğitim süresini azaltmak amacıyla veri setinde benzer eğilime sahip test verileri ayrılmıştır. Bu işlemler sonrasında Naive Bayes algoritması uygulanmıştır. Özetlemek gerekirse, Naive Bayes bütün koşullu olasılıkların çarpımı olarak düşünülebilir. Naive Bayes algoritmasının uygulanmasından sonra elde edilen sonucu incelediğimizde, başarı oranı yaklaşık 0,79 olmuştur. Naif Bayes algoritmasının hızlı çalışan istekli bir sınıflandırma algoritması olması, gerçek zamana yaklaşabilmesi ve aynı zamanda çok sınıflı tahmin özelliği için iyi çalışması özelliği ile tercih sebebi olmuştur. Zira bu çalışmada, hem savunma sistemleri hem de kullanılan veri seti gibi birçok sınıf vardır.

**Kaynakça**

<https://dergipark.org.tr/en/download/article-file/747619>

\* Arş. Gör. İstanbul Aydın Üniversitesi, Mühendislik Fakültesi, Yazılım Mühendisliği Bölümü,

cagdasozer@aydin.edu.tr, ORCID: 0000-0002-0581-7955

\*\* Arş. Gör. İstanbul Aydın Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü,

mustafatakaoglu@aydin.edu.tr, ORCID: 0000-0002-1634-2705