Marmara Fen Bilimleri Dergisi 2014,3:89-104
DOI: 10.7240/mufbed.24684

Makine Öğrenmesi Teknikleriyle Saldırı Tespiti: Karşılaştırmalı Analiz

Çetin KAYA[1], Oktay YILDIZ[2]

[1]Kara Harp Okulu Bilgisayar Mühendisliği Bölümü, 06654, Çankaya, ANKARA
[2]GaziÜniversitesi, Bilgisayar Mühendisliği Bölümü, 06570, Maltepe, ANKARA

Özet
İnternet, günlük hayatımızın vazgeçilmez bir parçasıdır. Artan web uygulamaları ve kullanıcı sayısı, veri güvenliği açısından bazı riskleri de beraberinde getirmiştir. Ağ güvenliği için önemli araçlardan biri olan saldırı tespit sistemleri, güvenli iç ağlara yapılan saldırıları ve beklenmeyen erişim taleplerini tespit etmede başarılı bir şekilde kullanılmaktadır. Günümüzde, pek çok araştırmacı, daha etkin saldırı tespit sistemi gerçekleştirilmesi amacıyla çalışma yapmaktadır. Bu amaçla literatürde farklı makine öğrenme teknikleri ile gerçekleştirilmiş pek çok saldırı tespit sistemi vardır. Yapılan bu çalışmada, saldırı tespit sistemlerinde sıklıkla kullanılan makine öğrenme teknikleri araştırılmış, kullandıkları sınıflandırıcılar, veri setleri ve elde edilen başarılar değerlendirilmiştir. Bu amaçla 2007-2013 yılları arasında SCI, SCI Expanded ve EBSCO indekslerince taranan ulusal ve uluslararası dergilerde yayınlanmış 65 makale incelenmiş, sonuçlar, karşılaştırılmalı bir şekilde sunulmuştur. Böylece, gelecekte yapılacak makine öğrenme teknikleri ile saldırı tespiti çalışmalarına bir bakış açısı kazandırılması amaçlanmıştır.

Anahtar kelimeler: STS, Makine öğrenmesi, KDD Cup99

Intrusion Detection with Machine Learning Techniques: Comparative Analysis

Abstract
The Internet is an indispensable part of our daily lives. The increasing number of web applications and the user, in terms of data security, has some risks. Intrusion detection systems, secure access to internal networks to detect attacks and unexpected due to the demands of one of the important tools for network security. In order to develop more effective intrusion detection systems a lot of investigative work. However, so many different machine learning techniques in the literature with intrusion-detection system. In this study, the intrusion detection systems are frequently used in machine learning techniques are researched, evaluated, and the resulting achievements classifiers, used by datasets. To this end between the years 2007-2013 65 article examined, the results are presented in a way that the comparative. Thus, the determination of the future machine learning techniques to gain a perspective on the work of the attack.

Keywords: IDS, Machine learning, KDD Cup99

1. Giriş
Günlük hayatımızın vazgeçilmez bir parçası olan internet Dünyada yaklaşık 2.7 milyar insan tarafından kullanılmaktadır [1]. Bankacılık sektöründen sağlık sektörüne, eğlenceden eğitime daha pek çok alanda yaygınlaşan internet uygulamaları, kullanıcı sayısını daha da arttırmaktadır. İnternet kullanımının her geçen gün yaygınlaşması beraberinde veri güvenliği sorununu ortaya çıkarmıştır. Veri güvenliği, verinin izinsiz erişimlerden, kullanımdan, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden korunması işlemidir. TS ISO/IEC 27001:2005 bilgi güvenliği yönetim sistemi standardı, bilgi güvenliğini üç başlık altında inceler. Bunlar;
Gizlilik: Bilgilerin yetkisiz erişimlere karşı korunmasıdır.
Bütünlük: Gönderici tarafından gönderilen verinin alıcıya herhangi bir değişikliğe uğramadan gönderilebilmesidir.
Erişilebilirlik: Bilgilere yetkili kişilerce erişilmek istendiğinde kullanıma hazır olmasıdır.

Sorumlu yazar/Corresponding author: Çetin KAYA Tel: 05436461179, e-posta: cetin78kaya@gmail.com

İnternet ortamında, ağa yönelik saldırı risklerinden dolayı, internet tabanlı saldırıları engellemek amacıyla güvenlik duvarı, anti virüs ya da saldırı tespit sistemleri gibi yazılımsal veya donanımsal araçlar tasarlanmıştır. Ağ sistemi, saldırganlardan ya da hackerlerden önemli verileri ve sistemleri korumak için bu güvenlik yazılımlarından bir ya da birkaçını kullanmaktadır. Tek başına bir güvenlik duvarı sistemine güvenmek, kurumsal ağlara ya da kişisel ağlara yönelik saldırıları engellemek için yeterli değildir. Bu nedenle, güvenlik duvarının açıklarını kapatmak için aynı zamanda saldırı tespit sistemi de kullanılır.

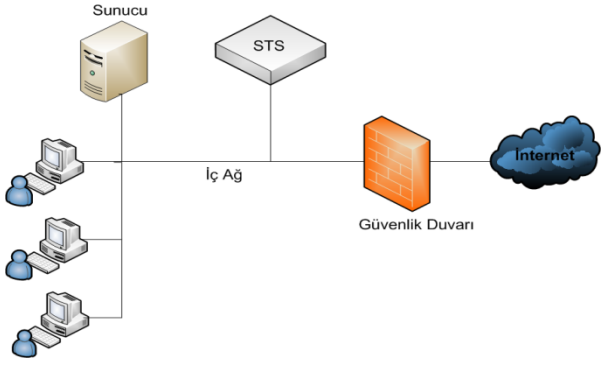
Saldırı tespit sistemi (STS), dış kaynaklardan gelen saldırılara karşı, bilgisayar ağında meydana gelen olayları otomatik olarak analiz eden yazılım veya donanımsal sistemlerdir [2]. Makine öğrenme teknikleri, saldırı tespit sistemlerinde başarılı bir şekilde kullanılmaktadır. Literatürde farklı makine öğrenme teknikleri ile gerçekleştirilmiş pek çok saldırı tespit sistemi vardır. Destek vektör makinesi (DVM), Bayes, Karar ağaçları, Yapay sinir ağları (YSA) en sık kullanılan makine öğrenme teknikleridir. Ancak son yılları kapsayan, farklı makine öğrenme tekniklerinin saldırı tespit sistemlerinde kullanılması ve performanslarının karşılaştırılması üzerine çok fazla çalışma bulunmamaktadır.

Yapılan bu çalışmada, 2007-2013 yılları arasında SCI, SCI Expanded, EBSCO gibi indekslerce taranan ulusal ve uluslararası dergilerde yayınlanmış 65 farklı makale incelenmiş, saldırı tespit sistemlerinde en sık kullanılan makine öğrenme teknikleri ve sonuçlar, karşılaştırılmalı bir şekilde sunulmuştur. Böylece, gelecekte yapılacak makine öğrenme teknikleri ile saldırı tespiti çalışmalarına bir bakış açısı kazandırılması amaçlanmıştır. Çalışma kapsamında incelenen makaleler Web of Science ve IEEE Xplore gibi veritabanlarında STS, makine öğrenmesi, makine öğrenmesi ile saldırı tespit sistemi, intrusion detection system based on machine learning, intrusion detection system based on bayes, intrusion detection system based on neural network, intrusion detection system based on SVM anahtar kelimeleri kullanılarak taranmıştır.

Makalenin ikinci bölümünde saldırı tespit sistemleri, üçüncü bölümünde makine öğrenmesi teknikleriyle saldırı tespiti ve yaygın kullanılan sınıflandırıcılardan bahsedilmiş son bölümde kullanılan veri setleri ve sonuçlarına yer verilmiştir.

2. Saldırı Tespit Sistemleri

İlk saldırı tespit sistemi konsepti Anderson tarafından 1980 yılında önerilmiştir [3]. Bace, saldırı tespit sisteminin görevini, bilgisayar sisteminde ya da ağ sisteminde gerçekleşen tüm olayları denetlemek ve kontrol etmek, güvenlik sorunları ortaya çıktığında ilgili personel ve birimleri uyarmak için alarm göndermek ve olası riskleri azaltmak için gerekli tedbirleri almak şeklinde tanımlamıştır. Saldırı tespit sisteminin çalışma döngüsünü bilgi toplama, analiz motoru ve cevap olarak üç başlık altında incelemiştir [4]. Şekil 1'de güvenlik önlemi olarak bir saldırı tespit sistemi görülmektedir.



Şekil 1: Saldırı Tespit Sistemi

Ağ üzerinden yapılabilecek saldırılar aşağıdaki gibi sıralanabilir.
Hizmet engelleme (Denial of Service-DOS): Bir sisteme, TCP/IP protokolünün yapısından kaynaklanan açıklardan faydalanılarak, sistemin tüm kaynaklarını tüketip hizmet veremez hale getirmek amacıyla arka arkaya yapılan düzenli saldırılardır. Hizmet aksatma saldırılarında bir veya birden fazla noktadan hedefteki bilgi sistemleri üzerine gereğinden fazla yükler bindirilerek, sistemler üzerindeki asli hizmetlerin aksaması ve bu aksama anında zayıflayan sistemlere sızabilmek amaçlanır. Disk alanlarının doldurulması, işlemci tüketimi, yerel alan ağlarındaki merkezi anahtarlara trafik yüklemek, internet yönlendiricilerine gereksiz trafik yükleyerek yetkisiz erişim elde etmek, hizmet aksatma saldırılarına örnek olarak verilebilir [5]. DOS saldırıları ağlar için en tehlikeli saldırılardan bir tanesidir. Çünkü ağ trafiğine bakarak DOS saldırılarının anlaşılması ve normal ağ trafiğinden ayırt edilmesi zordur. Bu saldırıların tespit edilebilmesi amacıyla anormallik tespiti tabanlı saldırı tespit sistemleri kullanılabilir [6].
Yönetici hesabını ele geçirerek yerel ağda oturum açma (Remote to Local-R2L): Kullanıcı yetkisine sahip olunmadığı halde, hedef ağdaki bilgisayara bazı paketler gönderilerek misafir ya da başka bir kullanıcı olarak bilgisayara erişim yetkisi kazanılmasıdır [6].
Kullanıcı hesabını yönetici hesabına yükseltme (User to Root-U2R): Kullanıcı hesabının yönetici hesabına yükseltilmesi saldırısı; sisteme erişim yetkisi olan fakat yönetici yetkilerine sahip olmayan bir kullanıcının yönetici haklarını elde etmesidir. Genellikle sistem açıklarını kullanarak gerçekleştirilir [6].
Bilgi tarama: Bilgi tarama saldırıları, bir sunucunun ya da herhangi bir makinenin geçerli ip adreslerini, ağdaki bilgisayar sayısını, bilgisayardaki kullanıcı sayısını ve kullanıcı bilgilerini, aktif giriş kapılarını (port) veya işletim sistemini öğrenmek için yapılırlar [6].
Saldırı tespit sistemleri, anormallik tespiti ve imza tabanlı olmak üzere ikiye ayrılır [7]. Anormallik tespiti tabanlı STS de, öncelikle sistemdeki kullanıcılar üzerinden normal davranışlar tanımlanır. Sisteme gelen her yeni istek normal veya anormal olarak sınıflandırılır. Bu yöntemin zorluğu, normal sistem özelliklerinin belirlenmesidir. Bu yöntemde yanlış veya yetersiz modelleme nedeniyle normal işlemler yanlışlıkla saldırı olarak kabul edilebilir. Bu yöntemin avantajı ise yeni saldırıların tespit edilebilmesidir [8]. İmza tabanlı STS ise, bilinen saldırıların imza kaydını tutar ve yeni gelen bir isteği kayıtlarını kontrol ederek "saldırı" ya da "normal davranış" olarak sınıflandırır.

3. Makine Öğrenme Teknikleriyle Saldırı Tespiti

Yapay zekânın bir branşı olan makine öğrenmesi, veriden karmaşık örüntünün tespit edilmesi ve akılcı karar verme için istatistik ve bilgisayarın hesaplama gücünden faydalanır. Makine öğrenme teknikleri sınıflandırma problemlerinde başarılı bir şekilde kullanılmaktadır [9, 10, 11, 12].
Literatürde, saldırı tespit sistemlerinde sıklıkla kullanılan makine öğrenme teknikleri aşağıdaki gibidir.

- Bayes sınıflama
- Destek vektör makinesi
- Karar ağaçları
- Yapay sinir ağları

3.1. Bayes Sınıflama

Bayes ağları, Makine öğrenmesinde öğreticili öğrenme alt başlığı altında incelenir [13]. Bayes sınıflandırma işleminde genel olarak elde bir örüntü (pattern) vardır ve bu örüntü daha önceden tanımlanmış olan sınıfları tespit eder. Gelen e-postalar içinde gereksiz iletilerin (spam) tespit edilmesi işlemi buna örnek olarak verilebilir. Bu örnekte; Spam e-posta ve spam olmayan e-posta iki sınıfı temsil eder. Elimizdeki spam ve spam olmayan e-postalardan yaralanarak gelecekte elimize ulaşacak e-postaların spam olup olmadığına karar verecek bir algoritma da öğreticili makine öğrenmesine örnektir [14].
Bayes teoremi, birden fazla etkenin olduğu bir olayın meydana gelmesinde, olayda hangi etkenin payının yüksek olduğunun hesaplanması temeline dayanır. Bayes teoremi aşağıda Eşitlik 1'de gösterildiği gibi ifade edilebilir.

$$\boldsymbol{P(e|T) = \frac{P(T|e)\,P(e)}{P(T)}} \qquad \textbf{(1)}$$

P(e) = e olayının önsel olasılığı
P(T) = T eğitim verisinin önsel olasılığı
P(T|e) = e olayı verildiğinde T'nin koşullu olasılığı
P(e|T) = T eğitim verisi verildiğinde e'nin koşullu olasılığı

Bayes sınıflandırıcılar, saldırı tespit sistemlerinde sıklıkla kullanılan bir yöntemdir. İncelenen çalışmalar Tablo 1' de gösterilmiştir. Bayes ile en yüksek sınıflandırma başarısı elde eden çalışmalar şunlardır: Farah Jemili ve arkadaşları [15] tarafından geliştirilen STS ile DARPA 99 veriseti kullanılarak elde edilmiştir. Yazarlar bu çalışmalarında DOS saldırılarında %99,62, bilgi tarama saldırılarında %100, U2R saldırılarında %98,63 ve R2L saldırılarında %42,62 doğrulukta başarı elde etmişlerdir. Dewan ve arkadaşları [16] ise KDD CUP99 verisetini kullanarak normal davranışları ayırt etmede %99,82, DOS saldırılarında %99,49, bilgi tarama saldırılarında %99,72, U2R saldırılarında %99,47 ve R2L saldırılarında %99,35 oranında bir başarı elde etmişlerdir.

3.2. Destek Vektör Makinesi

Destek Vektör Makinesi (DVM), Vapnik tarafından 1998 yılında önerilmiş güçlü bir sınıflandırıcıdır. Temeli istatistiksel yöntemlere dayanır. DVM, öğrenme alanında, elde edilen örüntüleri tanıma ve analiz etmede, sınıflama ve regresyon analizini kullanan denetimli bir öğrenme modelidir [17].
DVM, etiketli bir giriş veri setine ihtiyaç duyar. İki sınıftan oluşan verisetinde, girilen giriş veri setinden çıkış olarak iki sınıf oluşturur. Girilen eğitim örnekleri, iki kategoriden birine dahil edilir. DVM eğitim algoritması, yeni gelen bir örneği kategorilendirmek için bir model kurar. DVM modeli, uzayda noktalar gibi örneklerin temsilidir. Kategorilere ayrılan örnekler, mümkün olduğu kadar geniş, net bir hiperdüzlem ile ayrılır. Yeni örnekler aynı uzaya dâhil edilir ve hangi kategoriye ait oldukları tahmin edilir.
Saldırı tespit sistemlerinde DVM başarılı bir şekilde kullanılmaktadır. İncelenen çalışmalar Tablo 1' de gösterilmiştir. DVM ile en yüksek sınıflandırma başarısı elde eden çalışmalar şunlardır: 2010 yılında KDD CUP 99 veriseti kullanılarak yapılan çalışmada, Yongli Zhang ve arkadaşları [18] normal davranışları %99,32, DOS saldırılarını %93,81, bilgi tarama saldırılarını %33,67, U2R saldırılarını %39,31 ve R2L saldırılarını da %99,42 oranında doğru sınıflandırmayı başarmışlardır. Jun Wang ve arkadaşları [19] yapay arı kolonisi algoritması ve destek vektör makinesini ile KDD CUP 99 veri setini kullanarak normal davranışları ayırt etmede %100, DOS saldırılarını tespitte %99,92, bilgi tarama saldırılarında %100, U2R saldırılarında %76 ve R2L saldırılarında %87,92 oranında sınıflandırmayı başarmışlardır. Qi

Mu ve arkadaşları [20] ise DOS saldırılarını tespitte %100, bilgi tarama saldırılarında %100, U2R saldırılarında %100 ve R2L saldırılarında %99,11'lik bir başarı gözlemlemişlerdir.

3.3 Karar Ağaçları

Karar ağaçları, eğitim ve testinin hızlı olması, sonuçlarının daha kolay yorumlanabilmesi ve etkin olması sebebiyle sınıflandırmada sıklıkla kullanılan yöntemlerden biridir [21, 22]. Karar ağaçları ile sınıflandırma iki adımda gerçekleştirilir. İlk adımda ağaç oluşturulur. İkinci adımda bu ağaç yapısından sınıflandırma kuralları elde edilir. Genel olarak sınıflandırma işlemi şöyle ifade edilebilir: $D=\{t_1,t_2,\ldots, t_n\}$ bir veri tabanı olsun ve her bir kayıt t_i ile temsil edilsin. $C=\{C_1,C_2\ldots C_m\}$ ise m adet sınıftan oluşan sınıflar kümesini temsil etsin. Her bir C_j ayrı bir sınıftır ve her bir sınıf kendisine ait kayıtları içerir. Yani, $C_j=\{t_i|=C_j, 1\leq i\leq n$ ve $t_i \in D\}$, dir. Veritabanındaki her bir kayıt için alanlar ise $\{A_1,A_2,\ldots A_n\}$ 'den oluşsun. Bu tanıma ilaveten her bir kayıt $C=\{C_1,C_2,\ldots C_m\}$ sınıflarından birine ait ise karar ağacı şöyle tanımlanabilir: Her bir düğüm A_i alanı ile isimlendirilir. Kök düğüm ile yaprak arasındaki düğümler birer sınıflandırma kuralıdır.

Karar ağaçları oluşturulurken kullanılan algoritmanın ne olduğu önemlidir. Kullanılan algoritmaya göre ağacın yapısı değişebilir. Değişik ağaç yapıları farklı sınıflandırma sonuçları verebilir [23].

Karar ağaçlarına dayalı olarak geliştirilen birçok algoritma vardır. Bu algoritmalar birbirlerinden kök, düğüm ve dallanma kriterine göre farklı kategorilere ayrılırlar. Yaygın olarak bilinen algoritmalar ID3, C4.5 ve C5dir.

Literatürde Karar ağaçları ile gerçekleştirilmiş pek çok STS çalışması yer almaktadır. İncelenen çalışmalar Tablo 1' de gösterilmiştir. Karar ağaçları ile en yüksek sınıflandırma başarısı elde eden çalışmalar şunlardır; M. Bahrololum ve arkadaşları [24] normal davranışları ayırt etmede %99,96, DOS saldırılarını tespitte %99,97, bilgi tarama saldırılarında %99,66, U2R saldırılarında %88,33 ve R2L saldırılarında %99,02 oranında sınıflandırma başarısı elde etmişlerdir. Ayrıca 2012 yılında Ammar Alazab ve arkadaşları [25] KDD CUP 99 verisetini kullanarak normal davranışları ayırt etmede %98,2, DOS saldırılarını tespitte %97,2, bilgi tarama saldırılarında %99,6, U2R saldırılarında % 92,5 ve R2L saldırılarında %99,7 oranında başarı elde etmişlerdir. Karar ağaçları kullanılarak yapılan STS çalışmalarından bir diğeri 2013 yılında Vikas Sharma ve Aditi Nema [26] tarafından KDD CUP 99 veriseti kullanılarak gerçekleştirilmiştir. Sharma ve Nema, DOS saldırılarını tespitte %99,98, bilgi tarama saldırılarında %88,19, U2R saldırılarında % 51 ve R2L saldırılarında %94,70 oranında başarı elde etmişlerdir.

3.4. Yapay Sinir Ağları

Yapay Sinir Ağları (YSA), biyolojik sinir hücrelerine (nöron) modelleyen, güçlü bir sınıflandırma aracıdır. Ağı oluşturan her bir elemana yapay sinir (nöron) adı verilmektedir. Yapay sinir ağı çeşitli ağırlıklandırmalar sayesinde birbirine bağlanmış birçok yapay sinir hücresinden oluşmaktadır.

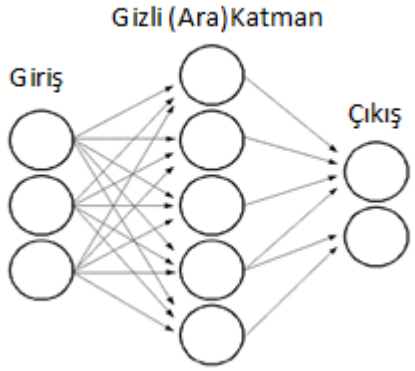
Normalde tek bir nöron sadece doğrusal problemleri çözebilir. Diğer birçok sınıflandırma problemini çözebilmek için çok katmanlı yapay sinir ağları, (Multi Layer Perceptron-MLP) kullanılmaktadır. Çok katmanlı YSA, fonksiyon uydurma, sınıflandırma ve eşleşme problemlerinde sıkça kullanılmaktadır. Sınıflandırmadaki başarısından dolayı STS'lerde sıklıkla kullanılmıştır [27].

Çok Katmanlı Algılayıcılar (ÇKA)'dan günümüzde en sık kullanılanı back propogation ağlardır. Bugün özellikle sınıflandırma işlemlerinde en çok kullanılan yöntemlerin başında

gelmektedir. Backpropogation ağlarda öğrenme fonksiyonu olarak delta öğrenme kuralı kullanılmaktadır. Delta öğrenme kuralı aşağıda gösterildiği gibi Eşitlik 2 ile ifade edilir.

$$\boldsymbol{w_{i,j}(new) = w_{i,j}(old) + (\mu * [t - f(y_{in})] * f'(y_{in}))} \qquad \textbf{(2)}$$

ÇKA'lar; girdi katmanı, ara katmanlar ve çıktı katmanı olmak üzere 3 katmandan oluşmaktadır. Bilgiler girdi katmanından ağa tanıtılır, ara katmanlardan çıktı katmanına ulaşır ve çıktı katmanından dış dünyaya aktarılır [28]. ÇKA mimarisi Şekil 2'de gösterilmiştir [29].
Yapay sinir ağı öğrenme sürecinde, gerçek hayattaki probleme ilişkin veri ve sonuçlardan diğer bir deyişle örneklerden faydalanılır. Probleme ilişkin değişkenler yapay sinir ağının girdi dizisini, bu değişkenlerle elde edilmiş gerçek sonuçlar ise yapay sinir ağının ulaşması gereken hedef çıktılar dizisini oluşturur.



Şekil 2: Standart üç katmanlı YSA yapısı

Öğrenme sürecinde, seçilen öğrenme yaklaşımına göre ağırlıklar değiştirilir. Ağırlık değişimi, öğrenmeyi ifade eder. YSA' da ağırlık değişimi yoksa, öğrenme işlemi de durmuştur. Bu nedenle eğitimde kullanılacak eğitim veri setinin oluşturulmasında çok dikkatli olunmalıdır. Veri setinin gerçekten de ilgili olayların motiflerini içerdiğinden emin olmak gerekir [29].
YSA kullanılarak gerçekleştirilen Saldırı Tespit Sistemlerinde oldukça başarılı sonuçlar elde edilmiştir. İncelenen çalışmalar Tablo 1' de gösterilmiştir. Guisong Liu ve arkadaşları [30], KDD Cup99 verisetini kullanarak HPCANN (Hierarchical Principal Component Analysis Neural Networks) ile STS geliştirmişler, normal davranışları %97,1, DOS saldırılarını %100, bilgi tarama saldırılarını %100 ve R2L saldırılarını da %97,2 başarı ile sınıflandırmışlardır. 2012 yılında; Xingchao Gong ve Xin Guan [31] KDD 99 verisetini kullanarak, normal davranışları %100, DOS saldırılarını %100, bilgi tarama saldırılarını %99,76, U2R saldırılarını %99,85 ve R2L saldırılarını da %99,88 oranında sınıflandırmayı başarmışlardır.

4. Makine Öğrenmesi Tekniklerinin Karşılaştırılması

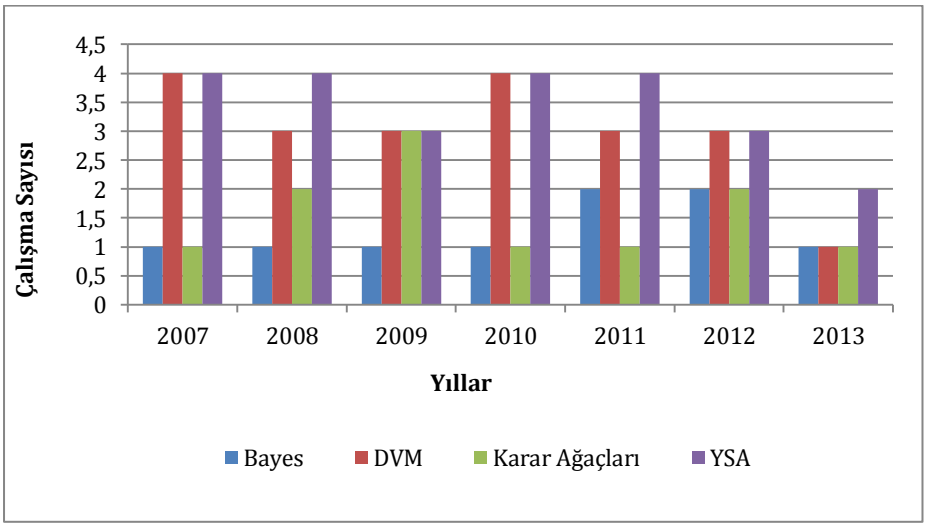
4.1. Sınıflandırıcılar

2007-2013 yılları arasında yapılan çalışmalar incelendiğinde bayes sınıflama, destek vektör makinesi, karar ağaçları ve yapay sinir ağlarının saldırı tespit sistemlerinde en sık kullanılan yöntemler olduğu görülmüştür. Tablo 1'de görüldüğü gibi bu sınıflandırıcılar içerisinde en çok tercih edilen yöntem YSA iken DVM en çok tercih edilen ikinci yöntem olmuştur.

Tablo1: İncelenmek üzere seçilen çalışmalar ve sınıflandırıcı türleri.

BAYES	DVM	KARAR AĞAÇLARI	YSA
9	**21**	**11**	**24**
F.Jemili vd. [15], Dewan Md. Farid ve Mohammad Zahidur Rahman [16], C. Xiang vd. [32], Farah Jemili vd. [33], Z. Muda vd. [34], W. Fan vd. [35], Hesham Altwaijry ve Saeed Algarny [36], Saurabh Mukherjee ve Neelam Sharma [37], Levent Koç vd. [38].	Yongli Zhang vd. [18], Jun Wang vd. [19], Qi Mu vd. [20] , Qiao Pei-li ve Chen Shi-feng [39], T. Shon ve J. Moon [40], Hua Zhou vd. [41], Yuan-Cheng Li ve Zhong-Qıang Wang [42], H. Li ve J. Wan [43], X. Ding vd. [44], Yuancheng Li vd. [45], Jing Ma vd. [46], Zhenguo Chen ve Guanghua Zhang [47], Hongle Du vd. [48], Huaping Liu vd. [49], Guan Xiaoqing vd. [50], Shi-Jinn Horng vd. [51], Preecha Somwang ve Woraphon Lilakiatsakun vd. [52], Guanghui Song et. al. [53], Liu Ning ve Zhao Jianhua [54], X. Yang ve Z. Yilai [55], A.M.Chandrasekhar ve K.Raghuveer [56].	M. Bahrololum vd. [24], A. Alazab vd. [25], Vikas Sharma ve Aditi Nema [26], S. Peddabachigari vd. [57], Joong-Hee Leet vd. [58], Shina Sheen ve R Rajesh [59], Wu vd. [60], Dai Hong ve Li Haibo [61], Yongjin Liu vd. [62], P. Sangkatsanee vd. [63], Manish Kumar vd. [64].	G. Liu vd. [30], X. Gong ve X. Guan [31], Hao-Ran Deng ve Yun-Hong Wang [65], Ling Yu vd. [66], P. G. Kumar ve D. Devaraj [67], R. Beghdad [68], S.T.Powers ve Jun He [69], Tie-Jun Zhou ve Li Yang [70], H. Karimi vd. [71], X. Han [72], B. Zhang ve Xuesong Jin Saeed [73], X. Tong vd. [74], Poojitha G. Vd. [75], G. Wang vd. [76], Dong-Xue Xia vd. [77], W. Huang ve L. Ju vd. [78], M. Govindarajan ve R.M. Chandrasekaran [79], L. Xiangmei ve Q. Zhi [80], B. Zhang [81], S.Devaraju ve S.Ramakrishnan [82], D. Ippoliti ve X. Zhou [83], X. Jiang vd. [84], Nidhi Srivastav ve Rama Krishna Challa [85], Liu Ning [86].

Şekil 3'de incelenen çalışmalarda kullanılan sınıflandırıcıların yıllar bazında dağılımı görülmektedir. Burada 2007, 2009, 2010 ve 2012 yılarında DVM ve YSA kullanım oranları eşit görülse de YSA'nın 2007-2013 yıları arasında en çok kullanılan sınıflandırıcı olduğu açıkça görülmektedir.



Şekil. 3 İncelenen çalışmalarda kullanılan sınıflandırıcıların yıllara göre dağılımı

Tablo 2'de görüldüğü gibi YSA, 2008, 2011 ve 2013'de en sık kullanılan sınıflandırıcı olmuştur. Bayes sınıflandırıcı ise en az tercih edilen sınıflandırıcıdır. Tablo 2'de yıllar bazında tercih edilen sınıflandırıcılar ve toplam çalışma sayısı görülmektedir.

Tablo 2 İncelenen çalışmalarda kullanılan sınıflandırıcı türlerinin yıllara göre dağılımı.

	07	08	09	10	11	12	13	Toplam
Bayes	1	1	1	1	2	2	1	9
DVM	4	3	3	4	3	3	1	21
Karar Ağaçları	1	2	3	1	1	2	1	11
YSA	4	4	3	4	4	3	2	24

4.2. Veriseti

Saldırı Tespit Sistemlerinin performansını belirlemek için en zorlu aşama geçerli ve uygun veri setlerinin elde edilmesidir. İnternet ortamından elde edilen veriler saldırının var olup olmadığına dair genel bir bilgi içermez. Saldırı için belirleyici özellik veya bilgi ağın gözlemlenmesi yoluyla elde edilebilir.

Genel olarak ağın gözlemlenmesi masraflı ve gereksiz bir iş olarak görülebilir. Ancak ağ veya bilgisayar sistemlerinin çalışabilmesi için, ağdan veya bilgisayar sistemlerinden veri toplama, artık günümüzde kaçınılmaz bir süreçtir. Bu süreç biraz maliyetli olduğundan dolayı bazı ağ mühendisleri yapay veriler kullanarak ağ veya sistemlerini sorunsuz çalıştırmayı istemektedirler. Ancak yapay verinin internet trafiğine benzediğini kanıtlamak zordur. Genel olarak; gerçek veri, saldırı türleri belli olan veri setleri bulmak ve ağ trafiğini tanımlamak ve benzetim yapmak zordur.

Yukarıda belirtilen zorluklara rağmen saldırı tespit sistemlerini test etmek için geçerli veri kümelerine ihtiyaç vardır. Genel olarak bir ağ trafiğini bir koklayıcı (sniffer) kullanarak gözlemlenebilir. Ancak sadece ağ paketlerini gözlemlemek ağ trafiği hakkında genel bir bilgi vermeyebilir. Bu dezavantajlara rağmen saldırı tespit sistemlerinin testleri için geliştirilen birkaç veri seti bulunmaktadır. Bunlardan bazıları KDD cup 99, DARPA 1998, DARPA 1999, UNM, SSCNNJU, CUCS, Windows sistem ve network tcpdump data verisetleridir.

KDD Cup'99 veriseti, basit, içerik, zaman tabanlı trafik ve host tabanlı trafik adı altında 4 farklı gruptan, 41 özellik, toplam 494.020 kayıttan oluşmaktadır.

KDD ve DARPA veriseti Amerikan Hava Kuvvetleri (US Air Force) network ağına benzer bir yapıya sahip olması düşünülerek tasarlanmış, bir benzetim verisetidir. KDD Cup99 ve DARPA veri seti saldırı tespit çalışmalarında en çok tercih edilen veri setidir [87].
2007-2013 yılları arasında yapılan çalışmalar incelendiğinde Tablo 3'de görüldüğü gibi DARPA98 ve UNM, en az tercih edilen veriseti iken, KDD Cup'99 veriseti en sık kullanılan veriseti olmuştur. Çok az çalışmada Tablo 3'de geçen veriseti dışında kendi verisetini kullanan çalışma vardır. Bunun nedeni bilgisayar ağ ve sistemlerinden veri toplamanın yüksek maliyetidir. Açık (public) verisetlerinin kullanılmasında diğer bir neden ise önerilen yaklaşımların, önceki çalışmalarla kıyaslanmak istenmesidir. Sonuç olarak public verisetleri makine öğrenme teknikleri ile STS çalışmalarında sıklıkla tercih edilen standart verisetleri olarak kabul gördüğü anlaşılmaktadır.

Tablo 3. İncelenen çalışmalarda kullanılan verisetlerinin yıllara göre dağılımı.

	07	08	09	10	11	12	13	Toplam
KDD Cup99	9	9	9	10	9	10	5	61
DARPA98	1							1
DARPA99	1	1						2
UNM					1			1

4.3. Performans Karşılaştırması

Tablo 4'de 2007-2013 yılları arasında yapılan çalışmalarda kullanılan verisetleri ve elde edilen genel sınıflandırma başarıları görülmektedir. Tablo 4'de açıkça görüldüğü gibi KDDCup99 veriseti kullanılarak gerçekleştirilen STS'de en yüksek başarı YSA ile %99,59 elde edilirken, en düşük başarı %93,72 ile bayes sınıflandırıcı ile elde edilmiştir. DARPA99 veriseti kullanılarak gerçekleştirilen STS'nde en yüksek başarı Bayes ile %98,03 elde edilirken, en düşük başarı %87,74 ile DVM 'le elde edilmiştir.

Tablo 4. İncelenen çalışmalarda kullanılan veriseti ve sınıflandırma başarısı.

	KDDCup99	DARPA99	DARPA98	UNM

Bayes	%93,72 [38]	%98,03 [33]	-	-
DVM	%99,44 [46]	%87,74 [40]	-	-
Karar Ağaçları	%99,33 [63]	-	%77,6 [58]	-
YSA	%99,59 [71]	-	-	%99,03 [79]

Tablo 5'de KDD cup99 veriseti ile yapılan testler sonucunda saldırı tiplerine göre elde edilen sınıflandırma başarıları görülmektedir. DOS tipi saldırılarda sınıflandırma başarıları birbirine yakın olmakla birlikte en yüksek başarı YSA ve DVM ile %100 elde edilmiştir. En düşük sınıflandırma başarı ise %99,62 ile Bayes sınıflandırıcı ile elde edilmiştir. Bilgi tarama saldırılarında, en yüksek sınıflandırma başarı oranı YSA, DVM ve Bayes sınıflandırıcı ile %100 elde edilmiştir. En düşük sınıflandırıcı ise %99,66 ile karar ağaçları olmuştur. R2Ltipi saldırılarda, en yüksek sınıflandırma başarı oranı YSA ile %100 elde edilmiştir. En düşük sınıflandırıcı ise %99,35 Bayes olmuştur. U2R tipi saldırılarda, en yüksek sınıflandırma başarı oranı DVM ile %100 elde edilmiştir. En düşük sınıflandırıcı ise %92,5 karar ağacı olmuştur.

Tablo 5. İncelenen çalışmalarda saldırı tiplerine göre sınıflandırıcıların başarısı.

	DOS	**Bilgi tarama**	**R2L**	**U2R**
Bayes	%99,62 [33]	%100 [33]	%99,35 [16]	%99,47 [16]
DVM	%100 [20]	%100 [19]	%99,42 [18]	%100 [20]
Karar Ağaçları	%99,98 [26]	%99,66 [24]	%99,70 [25]	%92,5 [25]
YSA	%100 [30]	%100 [30]	%99,88 [31]	%99,85 [31]

5. Sonuç ve Öneriler

Saldırı Tespit Sistemleri, halen üzerinde araştırma yapılması gereken önemli bir çalışma alanıdır. Daha etkin Saldırı Tespit Sistemi tasarlamak için Makine öğrenme teknikleri sıklıkla kullanılmaktadır. Yapılan bu çalışmada 2007-2013 yılları arasında makine öğrenme teknikleri kullanılarak gerçekleştirilmiş 65 farklı Saldırı Tespit Sistemi çalışması incelenmiş ve sınıflandırma performansları ve kullanılan verisetleri açısından karşılaştırılmıştır.

2007-2013 yılları arasında makine öğrenme teknikleri ile gerçekleştirilmiş STS'lerde en sık kullanılan yöntemin YSA ve KDD Cup 99'un da en sık kullanılan veriseti olduğu görülmüştür.

DOS, Bilgi tarama, R2Lve U2R tipi saldırıların tespitinde YSA yüksek başarı gösterirken, DVM ile DOS, Bilgi tarama ve U2R tipi saldırılarda etkin çözümler üretilebileceği

görülmüştür. Bayes ve Karar Ağaçları ile her ne kadar YSA ve DVM kadar başarılı sonuçlar elde edilemese de Bilgi tarama saldırılarında Bayes sınıflandırıcı, YSA ve DVM ile aynı oranda yüksek performans gösterebilmiştir.

Aşağıda vurgulanan bulgular, gelecekte Makine öğrenme teknikleri ile daha etkin saldırı tespit sistemi tasarlamak isteyen araştırmacılara faydalı olabilir.

- Tercih edilen sınıflandırıcı, geliştirilen STS'nin başarısında çok önemli rol oynar. YSA en sık kullanılan ve aynı zamanda en yüksek başarı oranını elde eden sınıflandırıcıdır. Ancak DVM da bazı saldırı tiplerinde etkin çözümler üretebilmektedir.
- Sistem eğitiminde ve test aşamasında kullanılan veriseti önemlidir. KDD Cup99 sıklıkla tercih edilen genel kullanıma açık (public) veriseti olmuştur. Elbette araştırmacılar kendi verilerini toplayabilir. Ancak bu hem maliyetli hem de ortaya konulan çalışmanın kıyaslanması açısından bazı sorunları gündeme getirecektir.
- Oluşturulan STS'nin başarısını ölçmek için yeteri kadar test verisine ihtiyaç vardır. Yeterli miktarda test verisi, sistem başarısının doğru ölçülmesinde önemli rol oynar. Ancak yine de önerilen STS ile elde edilmiş test sonuçları, gerçek ortamda aynı başarıyı vereceği anlamına gelmemektedir.

Kaynaklar

[1] «ICT Statistics Home Page» [Çevrimiçi], http://http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf. [30 04 2014 tarihinde erişilmiştir].

[2] X. Zhang, L. Jia, H. Shi, Z. Tang ve X. Wang, «The Application of Machine Learning Methods to Intrusion Detection,» 2012.

[3] J. Co, Computer Security Threat Monitoring and Surveillance, Pennsylvania: James P. Anderson Company, Fort Washington, 1980.

[4] R. Bace ve P. Mell, «NIST Special Publication on Intrusion Detection Systems,» *Publications of National Institute of Standards and Technology*, pp. 1-53, 2011.

[5] Y. Vural ve Ş. Sağıroğlu, «Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler,» *Gazi Üniv. Müh. Mim. Fak. Der.,* cilt 26, no. 1, pp. 89-103, 2011.

[6] K. Kendall, *Database of Computer Attacks for the Evaluation of Intrusion Detection Systems*, MIT Department of Electrical Engineering and Computer Science, 1999.

[7] K. Scarfone ve P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication, 2007, pp. 80-94.

[8] S. Axelsson, «Intrusion Detection Systems: A Survey and Taxonomy,» Department of Computer Engineering, Chalmers University of Technology, Sweden, 2000.

[9] D. Michie, D. Spiegelhalter ve C. Taylor, Machine Learning Neural and Statistical Classification, New York: Ellis Horwood Limited, 1994.

[10] F. Sebastiani, «Machine Learning in Automated Text Categorization,» *ACM Computing Surveys (CSUR)*, cilt 34, no. 1, pp. 1-47, 2002.

[11] J. Anderson, R. Michalski ve T. Mitchell, Machine learning: An artificial intelligence approach, M. Kaufmann, 1983.

[12] T. Nguyen ve G. Armitage, «A Survey of Techniques for Internet Traffic Classification Using Machine Learning,» *IEEE Communications Surveys and Tutorials*, cilt 10, no. 4, pp. 56-76, 2008.

[13] P. Domingos ve M. Pazzani, On the Optimality of the Simple Bayesian Classifier under Zero-One Loss, Springer, 1997.

[14] K. Çalış, O. Gazdağı ve O. Yıldız, «Reklam İçerikli Epostaların Metin Madenciliği Yöntemleri ile Otomatik Tespiti,» *Bilişim Teknolojileri Dergisi,* cilt 6, no. 1, 2013.

[15] F. Jemili, M. Zaghdoud ve M. Ben Ahmed, «A Framework for an Adaptive Intrusion Detection System using Bayesian Network,» *IEEE Intelligent and Security Informatics*, 2007.

[16] D. Farid ve M. Rahman, «Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm,» *Journal of computers,* cilt 5, no. 1, pp. 23-31, 2010.

[17] V. Vapnik, Statistical Learning Theory, New York: John Wiley, 1998.

[18] Y. Zhang ve Y. Zhu, «Application of Improved Support Vector Machines in Intrusion Detection,» %1 içinde *2nd International Conference on e-Business and Information System Security*, 2010.

[19] J. Wang, T. Li ve R. Ren, «A Real Time IDSs Based on Artificial Bee Colony Support Vector Machine Algorithm,» *Third International Workshop on Advanced Computational Intelligence*, 2010.

[20] Q. Mu, Y. Chen ve Y. Zhang, «Incremental SVM Algorithm to Intrusion Detection Base on Boundary Areas,» *International Conference on Systems and Informatics*, 2012.

[21] S. Wu ve W. Banzhaf, «The Use of Computational Intelligence in Intrusion Detection Systems:A Review,» *Applied Soft Computing,* cilt 10, no. 1, pp. 1-35, 2010.

[22] I. Witten ve E. Frank, Data Mining: Practical Machine Learning Tools and Techniques (Third Edition), Morgan Kaufmann Publication, 2011.

[23] M. Dunham, Data Mining Introductory and Advanced Topics, Prentice Hall Pearson Education Inc, 2003.

[24] M. Bahrololum, E. Salahi ve M. Khalegni, «Machine Learning Techniques for feature Reduction in Intrusion Detection Systems: A Comparison,» *Fourth International Conference on Computer Sciences and Convergence Information Technology*, 2009.

[25] A. Alazab, M. Hobbs, J. Abawajy ve M. Alazab, «Using Feature Selection for Intrusion Detection System,» *International Symposium on Communications and Information Technologies (ISCIT)*, 2012.

[26] V. Sharma ve A. Nema, «Innovative Genetic approach For Intrusion Detection by Using Decision Tree,» *International Conference on Communication Systems and Network Technologies (CSNT)*, 2013.

[27] C. Bitter, D. A. Elizondo ve T. Watson, «Application of Artificial Neural Networks and Related Techniques to Intrusion Detection,» *IJCNN*, 2010.

[28] S. Haykin, Neural Networks : A Comprehensive Foundation, New York: Macmillan College Publishing Company, 1999.

[29] R. P. Lippmann, «An Intoduction to Computing with Neural Nets,» *IEEE acoustic Speech and signal processing,* cilt 4, no. 2, pp. 4-22, 1987.

[30] G. Liu, Z. Yi ve S. Yang, «A Hierarchical Intrusion Detection Model Based on the PCA Neural Networks,» *Neurocomputing,* cilt 70, pp. 1561-1568, 2007.

[31] X. Gong ve X. Guan, «Intrusion Detection Model Based on the Improved Neural Network and Expert System,» *IEEE Symposium on Electrical & Electronics Engineering (EEESYM)*, 2012.

[32] C. Xiang, P. Yong ve L. Meng, «Design of multiple-level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees,» *Pattern Recognition*

Letters, cilt 29, pp. 918-924, 2008.

[33] F. Jemili, M. Zaghdoud ve M. Ben Ahmed, «Intrusion Detection based on Hybrid Propagation in Bayesian Networks,» *IEEE International Conference on Intelligence and Security Informatics,* 2009.

[34] Z. Muda, W. Yassin, M. Sulaiman ve N. Udzir, «Intrusion Detection based on K-Means Clustering and Naïve Bayes Classification,» *IAS 2011,* 2011.

[35] W. Fan, N. Bouguila ve D. Ziou, «Unsupervised Anomaly Intrusion Detection via Localized Bayesian Feature Selection,» *11th IEEE International Conference on Data Mining,* 2011.

[36] H. Altwaijry ve S. Algarny, «Bayesian Based Intrusion Detection System,» *Journal of King Saud University - Computer and Information Sciences,* cilt 24, no. 1, pp. 1-6, 2012.

[37] S. Mukherjee ve N. Sharma, «Intrusion Detection Using Naive Bayes Classifier with Feature Reduction,» *Procedia Technology,* cilt 4, pp. 119-128, 2012.

[38] L. Koc, T. Mazzuchi ve S. Sarkani, «A Network Intrusion Detection System Based on a Hidden Naïve Bayes Multiclass Classifier,» *Expert Systems with Applications,* cilt 39, pp. 13492-13500, 2013.

[39] Q. Pei-li ve C. Shi-feng, «Intrusion Detection System Technique Based on BP SVM,» *International Conference on Management and Service Science*, 2009.

[40] T. Shon ve J. Moon, «A Hybrid Machine Learning Approach to Network Anomaly Detection,» *Information Sciences,* cilt 17, pp. 3799-3821, 2007.

[41] H. Zhou, X. Meng ve L. Zhang, «Application of Support Vector Machine and Genetic Algorithm to Network Intrusion Detection,» *International Conference on Wireless Communications, Networking and Mobile Computing,*, 2007.

[42] Y. Li ve Z. Wang, «An Intrusion Detection Method Based on SVM and KPCA,» *International Conference on Wavelet Analysis and Pattern Recognition*, 2007.

[43] H. Li ve J. Wang, «Intrusion Detection System by Integrating PCNN and Online Robust SVM,» *International Conference on Network and Parallel Computing*, 2007.

[44] X. Ding, G. Zhang, Y. Ke, B. Ma ve Z. Li, «High Efficient Intrusion Detection Methodology with Twin Support Vector Machines,» *International Symposium on Information Science and Engineering,* 2008.

[45] Y. Li, Z. Wang ve Y. Ma, «An Intrusion Detection Method Based on KICA and SVM,» *7th World Congress on Intelligent Control and Automation,* 2008.

[46] J. Ma, X. Liu ve S. Liu, «A New Intrusion Detection Method Based on BPSO-SVM,» *International Symposium on Computational Intelligence and Design,* 2008.

[47] Z. Chen ve G. Zhang, «Support Vector Machines Improved by Artificial Immunisation Algorithm for Intrusion Detection,» *International Conference on Information Engineering and Computer Science,* 2009.

[48] H. Du, S. Teng, X. Fu, W. Zhang ve Y. Pu, «A Cooperative Intrusion Detection System Based on Improved Parallel SVM,» *Joint Conferences on Pervasive Computing ,* 2009.

[49] H. Liu, Y. Jian ve S. Liu, «A New Intelligent Intrusion Detection Method Based on Attribute Reduction and Parameters Optimization of SVM,» *Second International Workshop on Education Technology and Computer Science,* 2010.

[50] G. Xiaoqing, G. Hebin ve C. Luyi, «Network Intrusion Detection Method Based on Agent and SVM,» *The 2nd IEEE International Conference on Information Management and Engineering,* 2010.

[51] S. Horng, M. Su, Y. Chen, T. Kao, R. Chen, J. Lai ve C. Perkasa, «A Novel Intrusion

Detection System Based on Hierarchical Clustering and Support Vector Machines,» *Expert Syst. Appl,* cilt 38, no. 1, pp. 306-313, 2011.

[52] P. Somwang ve W. Lilakiatsakun, «Computer Network Security Based On Support Vector Machine Approach,» *11th International Conference on Control, Automation and Systems,* 2011.

[53] G. Song, J. Guo ve Y. Nie, «An Intrusion Detection Method based on Multiple Kernel Support Vector Machine,» *International Conference on Network Computing and Information Security*, 2011.

[54] L. Ning ve Z. Jianhua, «Intrusion Detection Research Based on Improved PSO and SVM,» *International Conference on Automatic Control and Artificial Intelligence*, 2012.

[55] X. Yang ve Z. Yilai, «An Intelligent Anomaly Analysis for Intrusion Detection based on SVM,» *International Conference on Computer Science and Information Processing*, 2012.

[56] A. Chandrasekhar ve K. Raghuveer, «Intrusion Detection Technique by Using k Means, Fuzzy Neural Network and SVM Classifiers,» *International Conference on Computer Communication and Informatics,* 2013.

[57] S. Peddabachigari, A. Abrahamb, C. Grosanc ve J. Thomas, «Modeling Intrusion Detection System Using Hybrid Intelligent Systems,» *Journal of Network and Computer Applications,* cilt 30, pp. 114-132, 2007.

[58] J. Leet, J. H. Leet, S. G. Sohn ve J. H. Ryu, «Effective Value of Decision Tree with KDD 99 Intrusion Detection Datasets for Intrusion Detection System,» *10th International Conference on Advanced Communication Technology,* 2008.

[59] S. Sheen ve R. Rajesh, «Network Intrusion Detection Using Feature Selection and Decision Tree Classifier,» %1 içinde *IEEE Region 10 Conference, TENCON,* 2008.

[60] S. Y. Wu ve E. Yen, «Data mining-based intrusion detectors,» *Expert Systems with Applications,* cilt 36, no. 3, pp. 5605-5612, 2009.

[61] D. Hong ve L. Haibo, «A Lightweight Network Intrusion Detection Model Based on Feature Selection,» *15th IEEE Pacific Rim International Symposium on Dependable Computing*, 2009.

[62] Y. Liu, N. Li, L. Shi ve F. Li, «An Intrusion Detection Method Based on Decision Tree,» *International Conference on E-Health Networking, Digital Ecosystems and Technologies*, 2010.

[63] P. Sangkatsanee, N. Wattanapongsakorn ve C. Charnsripinyo, «Practical Real-Time Intrusion Detection Using Machine Learning Approaches,» *Computer Communications,* cilt 34, pp. 2227-2235, 2011.

[64] M. Kumar, M. Hanumanthappa ve T. V. Kumar, «Intrusion Detection System Using Decision Tree Algorithm,» *14th International Conference on Communication Technology (ICCT)*, 2012.

[65] H. R. Deng ve Y. H. Wang, «An Artificial-Neural Network-Based Multiple Classifiers Intrusion Detection System,» *Proceedings of the 2007 International Conference on Wavelet Analysis and Pattern Recognition*, 2007.

[66] Y. Yu, B. Chen ve J. Xiao, «An Integrated System of Intrusion Detection Based on Rough Set and Wavelet Neural Network,» *Third International Conference on Natural Computation*, 2007.

[67] P. G. Kumar ve D. Devaraj, «Network Intrusion Detection Using Hybrid Neural Networks,» *International Conference on Signal Processing, Communications and Networking*, 2007.

[68] R. Beghdad, «Critical Study of Neural Networks in Detecting Intrusions,» *Computers & Security,* cilt 27, pp. 168-175, 2008.

[69] S. T. Powers ve J. He, «A Hybrid Artificial Immune System and Self Organising Map for Network Intrusion Detection,» *Information Sciences,* cilt 178, pp. 3024-3042, 2008.

[70] T. J. Zhou ve L. Yang, «The Research of Intrusion Detection Based on Genetic Neural Network,» *International Conference on Wavelet Analysis and Pattern Recognition,* 2008.

[71] H. Karimi, M. A. Montazeri ve M. D. Jazi, «A New Approach for Detecting Intrusions Using Jordan/Elman Neural Networks,» *First International Conference on Complexity and Intelligence of the Artificial and Natural Complex Systems. Medical Applications of the Complex Systems. Biomedical Computing, CANS'08* , 2008.

[72] X. Han, «An Improved Intrusion Detection System Based on Neural Network,» *Intelligent Computing and Intelligent Systems,* cilt 1, pp. 887-890, 2009.

[73] B. Zhang ve X. J. Saeed, «A Joint Evolutionary Neural Network for Intrusion Detection,» *Information Engineering and Computer Science,* pp. 1-4, 2009.

[74] X. Tong, Z. Wang ve H. Yu, «A Research Using Hybrid RBF/Elman Neural Networks for Intrusion Detection System Secure Model,» *Computer Physics Communications,* cilt 180, pp. 1795-1801, 2009.

[75] G. Poojitha, K. N. Kumar ve P. J. Reddy, «Intrusion Detection Using Artificial Neural Network,» *Second International conference on Computing, Communication and Networking Technologies* , 2010.

[76] G. Wang, J. Hao, J. Mab ve L. Huang, «A New Approach to Intrusion Detection Using Artificial Neural Networks and Fuzzy Clustering,» *Expert Systems with Applications,* cilt 37, pp. 6225-6232, 2010.

[77] D. X. Xia, S. H. Yang ve C. G. Li, «Intrusion Detection System based on Principal Component Analysis and Grey Neural Networks,» *Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, 2010.

[78] W. Huang ve L. Ju, «Intrusion Detection Method Based On Sparse Neural Network,» *International Conference on Multimedia Technology (ICMT)*, 2010.

[79] M. Govindarajan ve R. M. Chandrasekaran, «Intrusion Detection Using Neural Based Hybrid Classification Methods,» *Computer Networks,* cilt 55, pp. 1662-1671, 2011.

[80] L. Xiangmei ve Q. Zhi, «The Application of Hybrid Neural Network Algorithms in Intrusion Detection System,» *International Conference on E -Business and E - Government (ICEE)*, 2011.

[81] B. Zhang, «A Heuristic Genetic Neural Network for Intrusion Detection,» *International Conference on Internet Computing and Information Services (ICICIS)*, 2011.

[82] S. Devaraju ve S. Ramakrishnan, «Performance Analysis of Intrusion Detection System Using Various Neural Network Classifiers,» *International Conference on Recent Trends in Information Technology (ICRTIT),* 2011.

[83] D. Ippoliti ve X. Zhou, «A-GHSOM: An Adaptive Growing Hierarchical Self Organizing Map for Network Anomaly Detection,» *Parallel Distrib. Comput.,* cilt 72, pp. 1576-1590, 2012.

[84] X. Jianga, K. Liub, J. Yana ve W. Chen, «Application of Improved SOM Neural Network in Anomaly Detection,» *Physics Procedia,* cilt 33, pp. 1093-1099, 2012.

[85] N. Srivastav ve R. K. Challa, «Novel Intrusion Detection System integrating Layered Framework with Neural Network,» *3rd International Advance Computing Conference (IACC)*, 2013.

[86] L. Ning, «Network Intrusion Classification Based on Probabilistic Neural Network,» *International Conference on Computational and Information Sciences,* 2013.

[87] M. Tavallaee, N. Stakhanova ve A. A. Ghorbani, «Toward Credible Evaluation of Anomaly-Based Intrusion-Detection Methods,» *Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews,* cilt 40, no. 5, pp. 516-524, 2010.