Beykoz Akademi Dergisi, 2022; 10(1), 78-87 ARAŞTIRMA MAKALESİ
Gönderim tarihi: 29.11.2021 Kabul tarihi: 25.05.2022
DOI: 10.14514/BYK.m.26515393.2022.10/1.78-87

YAPAY ZEKÂ TEKNİKLERİNİN SALDIRI TESPİT SİSTEMLERİ'NDE KULLANIMI

Mahbub Dilan KOYUNCU[1], Nafiz ÜNLÜ[2]

Öz

Teknoloji kullanımının yaygınlaşması ile internet ve diğer ağlara birden çok bağlantı noktasının olduğu, farklı kanallardan gelebilecek tehditlerin artış gösterdiği gözlemlenmiştir. Mevcut sistemlerde, tehditlerin tespit ve bertaraf edilmesi için kullanılan güvenlik duvarı, şifreleme tekniklerinin yeterli olmaması mevcut ağ sistemlerine farklı tespit ve önleme sistemlerinin kullanılmasına yol açmış, Saldırı Tespit Sistemleri de bu ihtiyaçtan yola çıkılarak tasarlanmıştır. Geleneksel olarak isimlendirebileceğimiz imza ve anomali tabanlı Saldırı Tespit Sistemleri değişen ve gelişen teknolojik gelişmeler karşısında durağan kalmış, daha çok anlık çalışabilecek, saldırıları daha hızlı ve yüksek oranlarda doğru tespit edebilecek, insan faktörünün daha az yer aldığı bir sisteme geçilmesi önem kazanmış, bu maksat ile Yapay zekâ teknolojilerinin Saldırı Tespit Sistemlerinin tasarımında etkin rol alması kaçınılmaz olmuştur.

Anahtar Kelimeler: Saldırı Tespit Sistemleri, Yapay zekâ teknolojileri, Tehdit

JEL Sınıflandırması: O30, O32, O33

USE OF ARTIFICIAL INTELLIGENCE TECHNIQUES IN INTRUSION DETECTION SYSTEMS

Abstract

With the widespread use of technology, it has been observed that there are multiple connection points to the internet and other networks, and threats from different channels have increased. In existing systems, the inadequacy of firewall and encryption techniques used to detect and eliminate threats has led to the use of different detection and prevention systems in existing network systems, and Intrusion Detection Systems have been designed based on this need. Signature and anomaly- based Intrusion Detection Systems, which we can call traditional, have remained stagnant in the face of changing and developing technological developments, it has gained importance to switch to a system that can work more instantaneously, can detect attacks faster and at higher rates, and where the human factor is less. It has been inevitable for intelligence technologies to take an active role in the design of Intrusion Detection systems.

Keywords: Intrusion Detection System, Intelligence Technologies, Attacks

JEL Classification: O30, O32, O33

[1]İstanbul Teknik Üniversitesi, Bilişim Enstitüsü, Siber Güvenlik, koyuncuma@itu.edu.tr, ORCID: 0000-0002-0516-6179

[2]Dr.Öğr. Üyesi, İstanbul Teknik Üniversitesi, Bilişim Enstitüsü, Siber Güvenlik, unluna@itu.edu.tr, ORCID: 0000-0002-2094-8080

Beykoz Akademi Dergisi, 2022; 10(1), 78-87 ARAŞTIRMA MAKALESİ
Gönderim tarihi: 29.11.2021 Kabul tarihi: 25.05.2022
DOI: 10.14514/BYK.m.26515393.2022.10/1.78-87

1. Giriş

Teknolojinin hızla gelişmesi ile internet ilk kullanım alanı olan askeri alandan, kamu alanına hızlı bir geçiş yapmış, kamu alanındaki kullanımı ile de sınırlı kalmayarak bireysel alan içerisinde hatırı sayılır bir mevki kazanmıştır. Bireysel alanda kullanıma başlamasıyla birlikte internet yayılım hızı ivme kazanmış, 2021 yılında TUİK tarafından hazırlanan hane halkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre 2021 yılında hanelerin %92'sinin internete erişim imkânın bulunduğu, bu oranın 2020 yılında ise %90,7 olduğu görülmüştür (TUİK, 2021).

Şekil 1. Hane Halkı Bilişim Teknolojileri Kullanım Araştırması

Bilgisayar ağı teknolojisinin uygulama kapsamının sürekli genişlemesiyle birlikte, İnternet aralığında var olan çeşitli kötü niyetli saldırılar, bilgisayar kullanıcılarına ve ağ kaynaklarına ciddi zararlar vermiştir. Siber Saldırı olarak isimlendirilen bu tehditler gizli ve hassas bilgilere erişilmesi veyahut bir veya birden fazla bilgisayardan karşıdaki bilgisayarlara veya ağlara yapılan veri çalmak, değiştirmek ya da yok etmek için çeşitli yöntemler kullanılarak yapılan saldırı eylemlerinin bütününe verilen isimdir. Politik nedenler, Meydan okuma, Web sitelerinden intikam alma isteği, Vatanperverlik/Milliyetçilik düşüncesi, Maddi kazanç elde etme isteği vb. sebepleri ile gerçekleştirilen bu saldırılar hem maddi hem de itibar açısında kurum ve kuruluşlara geri dönülmez zararlar verebilmektedir.

Kasperky tarafından 2020 yılı özelinde yapılan araştırmaya göre web tehditlerini tespit etmede kullanılan teknolojilerin engellediği ortalama web saldırısı sayısı da %25 oranında arttığı gözlenmiştir. Tüm tehditlerin sayısında artış gözlendiği, engellenen web saldırılarının çoğunun ise kullanıcıları kimlik avı sitelerine yönlendiren saldırılar olduğu tespit edilmiştir (Anonim, 2020).

Ağlara ve sistemlere yapılan siber saldırıların son yıllarda bu denli artmasının nedenleri düşünüldüğünde, dünya genelinde hemen hemen her konuda olduğu gibi internet kullanımının da globalleşmesi, mevcut kurum ve kuruluşların dağınık sistemler şeklinde, çok bileşenli sistemlerin bulunması, tehdit unsuru olan ve bilgisayar korsanı olarak adlandırılan saldırganların ağ yapılarını, sistemleri hızlı öğrenmesi, saldırı araçlarının otomatikleştirilmesi ile saldırıların daha kolay yapılabilmesi, geliştirilen yeni yazılım ve donanım sistemlerinin zayıflıklarından kaynaklanan güvenlik açıklarının mevcut olması vb. unsurların etkin olacağı görülmektedir.

Beykoz Akademi Dergisi, 2022; 10(1), 78-87 ARAŞTIRMA MAKALESİ
Gönderim tarihi: 29.11.2021 Kabul tarihi: 25.05.2022
DOI: 10.14514/BYK.m.26515393.2022.10/1.78-87

Ağ yapılarına ve bilgisayar sistemlerine karşı yapılan siber tehditlerin tespit edilmesi, bilgisayar ve ağ sistemlerine ilk giriş noktalarında bertaraf edilebilmesi, gerektiğinde bu bilgilerin gelecek dönemlerdeki saldırıları tahmininde kullanılması maksadıyla güvenlik duvarları, şifreli yapılar kullanılmaya başlanmıştır. Fakat özellikle sosyal mühendislik yöntemleri kullanılarak aşılan bu yöntemlerin eksikliklerinin bulunduğu görülmüş, otomatikleşmiş, saldırı tespitinde doğru saptamaları yapabilecek Saldırı Tespit Sistemleri'nin tasarlanması söz konusu olmuştur. Saldırı Tespit Sistemi, saldırı uyaranlarının yorumlanma süreci olarak tanımlanır ve bir bilgisayar sisteminde veya ağda meydana gelen durumların gözlenerek, dersler çıkarılarak bilginin mahremiyetini, bütünlüğünü ve erişilebilirliğini bozmak ya da sistemin güvenlik mekanizmalarını atlatmak için yapılan bir dizi komutlar olarak göz önüne çıkar. Saldırı Tespit Sistemleri, sisteme olan saldırılar sonucunda sistem içerisinde meydana gelen anomalileri, kötü amaç ile kullanılan işlemlerin tespiti yaparak daha sonra olabilecek saldırılara karşı bir önlem oluşturmaya çalışmaktadır. Saldırı Tespit Sistemleri temelde yazımızda da ilgileneceğimiz üzere tespit yöntemlerine göre farklı isimler almaktadır (Yıldız ve Arıcı, 2010).

2. Saldırı Tespit Sistemlerinin Yapısal İncelemesi

Saldırı Tespit Sistemleri temel olarak İmza Tabanlı ve Anomali Tespiti yapan sistemler olarak iki ana yapıdan oluşmaktadır.

2.1. İmza Tanıma Temelli veya Kötüye Kullanım yolu ile Saldırı Tespiti

Ağlarda meydana gelen saldırıların karakteristiğini oluşturarak bir anlamda saldırı yapan unsurun bir imzasını çıkararak daha sonra aynı saldırı unsuru tarafından gelebilecek saldırıları saptama için kullanılan bir yöntemdir. Bu yöntemin kullanılmasında, saldırgan daha önce kullandığı saldırı yöntemleri bir veri seti ki bu veri setinin oluşturulmasında istatistik biliminden faydalanılmaktadır, haline getirilerek kurallar oluşturulmakta, dışarıdan ağ sistemine yeni gelen her bir davranış, bu kural seti ile karşılaştırılarak aynı tip bir saldırı olup olmadığı belirlenmektedir.

Eğer ağa dışarıdan yeni gelen davranış mevcut saldırı veri setleri ile benzeşiyorsa saldırı olarak nitelendirmektedir. Fakat söz konusu davranış, eğer mevcut veri setleri ile uyuşmuyorsa saldırı olarak nitelendirilmez. Bu durum saldırı niteliğinde olan, sadece veri setimize uymadığı için saldırı olmadığına karar verebildiğimiz bir ikileme sürüklenmemize sebebiyet verebilmektedir (Frank, 1994).

2.2. Anomali Tabanlı Saldırı Tespiti

Anomali Tabanlı Saldırı Tespitinde mevcut ağ trafiğinin izlenmesi sürecin en önemli parçasıdır. Durgun ve normal olarak adlandırabileceğimiz ağ üzerindeki farklılıkları yani "anomalileri" izlemek söz konusu ağ üzerindeki saldırıların tespitini kolaylaştıracaktır.

Anomali Tabanlı Saldırı Tespiti yönteminde esasında "normal" olan durumun karakteristiği çıkarılır ve bu "normal" durum haricindeki durumlar ki bunlar anomali olarak adlandırılır saldırı olarak nitelendirilmektedir. Bu tespit yöntemi ile daha geniş bir aralıktaki saldırıların tespiti kolaylaşırken, esasında saldırı olmayan davranışlar da saldırı olarak etiketlenebileceği gözlemlenmiştir.

Gönderim tarihi: 29.11.2021 Kabul tarihi: 25.05.2022
DOI: 10.14514/BYK.m.26515393.2022.10/1.78-87

Son yıllarda ağ ve bilgisayar sistemlerine yapılan saldırıların artması ve çeşitlenmesi siber güvenlik alanında çalışmalar yapan insanlar tarafından bahsi geçen iki ana Saldırı Tespit Sistemleri için iyileştirmeler yapılmasını zorunlu kılmıştır. Özellikle daha önce tespit edilmeyen türde bir saldırıyı bertaraf etmek önemli bir dayanak haline gelmiş, bu saikle Anomali Tabanlı Saldırı Tespit Sistemlerinin temel yapı olarak alınarak, yapay zekâ yöntemleri ile harmanlanması, bu sayede insan unsurunu elimine eden, başarı oranı yüksek, kendi kendine öğrenebilen, yüksek performans ile çalışan, düşük hata oranları ile işlem yapabilen Saldırı Tespit Sistemlerinin tasarlanması ön plana çıkmıştır. İşbu yazıda yapay zekâ hakkında kısa bir bilgi verilerek, yapay zekânın Saldırı Tespit Sistemlerindeki kullanım yöntemlerinin bir derlemesi yapılacaktır (Tanrıkulu, 2009).

3. Yapay Zekâ ve Saldırı Tespit İlişkisi

Yapay zekâ, insan düşünce biçimini temel alarak, insanlar tarafından yapılabilen tüm görevleri insanlar kadar ve bazı durumlarda insanlardan daha iyi yerine getirebilen yetenekli yazılım ve sistemlerin genel adıdır. Yapay zekâ özellikle gelişen teknoloji ve bununla birlikte artışa geçen siber saldırıların önlenmesi için yardımcı unsurlar olarak görülebilirler. Siber teknoloji alanında en başta makine öğrenmesi olmak üzere, sinir ağları, akıllı ajanlar, bulanık mantık, yapay bağışıklık sistemleri, veri madenciliği, patern tanıma vb. benzer yöntemler kullanılmaktadır.

Yapay zekâ, temel olarak insan düşünce biçimi ile örtüşebilen, sadece verilen komutlar ile değil, kendi işlevleri ile de hareket edebilen güçlü yapay zekâlar ve sadece verilen veriler ışığında çıkarım yapabilen, bütünleşik bir düşünce biçimine sahip olmayan zayıf yapay zekâlar olmak üzere iki ayrı yapıda incelenebilir. Günümüzdeki amaç güçlü yapay zekâları hayata geçirmek olmak ile birlikte, halen zayıf yapay zekâların kullanılmakta olduğu görülebilir (Dilek ve ark., 2015).

Saldırı Tespit Sistemleri, siber saldırılarda ilk savunma mekanizmalardan biri olarak karşımıza çıkmaktadır. Siber savunma ortamı içerisinde engelleyici bir unsur olması bakımından, özellikle büyük kurum ve kuruluşlar, devletler ve askeri sistemlerin büyük ve karmaşık siber altyapılarının korunmasında etkin olarak Saldırı Tespit Sistemleri kullanılmaktadır. Gelişen teknoloji ile sayıca artış gösteren ağ sistemleri, bağlantı noktaları saldırganlar için çekici hale gelmiştir. Saldırı Tespit Sistemlerinin bu karmaşık yapıya sahip ağ yapılarının korunmasında en önemli gücü sistem büyük ölçüde zarar görmeden, saldırganın etkisi tüm noktalara ulaşmadan ve geri dönülemez bir altyapı kaybı yaşamadan önce saldırıyı tespit edebilmesidir. Saldırı Tespit Sistemleri devlet ve askeri ağ sistemleri gibi kritik, özel ve riskli bilgiler içeren verilerin korunmasında, bu verilere karşı yapılacak gelecek saldırıların da karakteristiğini ve teknik yapısını çıkarmak için kullanılabilmektedirler.

Saldırı Tespit Sistemleri siber saldırıların bertaraf edilmesinde etkin bir rol almakta fakat saldırganların bir adım önde hareket etmeleri nedeniyle bazı durumlarda saldırıları tamamen ortadan kaldıramamaktadır. Bunun en büyük sebebi olarak özellikle geleneksel Saldırı Tespit Sistemlerinin sınırlı bir veri ve yazılıma sahip olmaları, yeterince hızlı karar verememeleri, anlık ve proaktif olarak saldırıyı tespit etmekte güçlük yaşamaları verilebilir. Bu noktada akıllı bir algoritma ile tasarlanmış, değişen saldırıları erkenden algılayabilecek yapay zekânın kullanıldığı Saldırı Tespit Sistemleri görevi devralmaktadır.

Günümüz teknolojisinde yapay zekâ algoritmaları ve Saldırı Tespit Sistemleri iki farklı yapı ile birlikte çalışmaktadır.

Gönderim tarihi: 29.11.2021 Kabul tarihi: 25.05.2022
DOI: 10.14514/BYK.m.26515393.2022.10/1.78-87

Bunlardan ilki "analist yönlendirmeli" bir diğeri ise "makine öğrenmeli" yapılardır. Bu iki yapının temel farkı sınıflara ayrılmış, etiketlenmiş veriler ile eğitilen sistemler analist yönlendirmeli olarak isimlendirilirken, daha önceden herhangi bir şekilde üzerinde çalışılmamış, bilinmeyen veri setleri kullanılarak bağlantılar bulmaya, birbiriyle ilişkili olan verileri kategorize etmeye çalışan sistemler ise makine öğrenmeli yapılar olarak isimlendirilirler.

Her yapıda olduğu gibi bu iki yapının kullanılmasının da bazı avantaj ve dezavantajları bulunmaktadır. Makine öğrenmeli yapay zekâ algoritmasının kullanılması, yeni ve daha önce karşılaşılmamış saldırıların tespitinde kolaylık sağlarken, analist tabanlı yapay zekâ algoritmaları bir davranışın daha önceki saldırılardan biriyse yüksek oranda saldırıyı tespit edebilmektedir. Bunun yanı sıra makine öğrenmeli yapay zekâ algoritması kullanılması, esasen saldırı olmayan veyahut saldırıyken saldırı olarak etiketlenmeyen davranışların meydana gelmesine sebebiyet verebilirken, analist tabanlı yapay zekâ algoritmalarında ise daha önce karşılaşılmamış saldırıların tespit edilememesi söz konusu olabilmektedir. Her iki yapay zekâ algoritmasında da büyük bir çaba gerektiren saldırı ve normal davranış analizlerinin yapılması yorucu ve uzun süreli olabilmekte, doğru olarak tanımlanmış veri setlerinin olmasını zorunlu kılmaktadır. Buna ek olarak araştırma sürecinin sınırlı bir zaman zarfı ve maddi kısıtlar içermesi sistemlerin, değişen ve gelişen saldırganların hızına bahsedilen sebeplerden ötürü yetişilememesi en önemli dezavantajlar olarak görülebilmektedir (Veeramachaneni ve ark., 2016).

4. Saldırı Tespit Sistemlerinde Kullanılan Yapay Zekâ Algoritma Yapıları

Yapay Zekâ algoritmalarının Saldırı Tespit Sistemlerinde kullanılmasının hız, performans, doğru belirlenmiş saldırı tespiti konularında önemli ayrıcalıklar kazandıracağı görülebilmektedir. Yapay zekâ algoritması denildiğinde farklı altyapı sistemleri ve öğrenme biçimleri kullanılmakta olup aşağıda en çok kullanılan Yapay Zekâ algoritmalarına yer verilmiştir (Haq ve ark., 2015).

I. Bayes Sınıflama
II. Destek Vektör Makinesi
III. Karar Ağaçları
IV. Yapay Sinir Ağları
V. Uzman Sistemler
VI. Akıllı Ajanlar
VII. Arama Yöntemi

4.1. Bayes Sınıflama

Bayes sınıflandırma yöntemi, analist yönlendirmeli yapay zekâ sınıfına girmektedir. Bu yöntem için mevcut sistemin elinde bir karakteristik bulunmakta olup, bu karakteristik benzeri davranışların tespit edilmesi için kullanılmaktadır. Bu yönteme verilebilecek en iyi yöntem spam e-posta olarak adlandırdığımız e-posta içeriğidir. Sistem bünyesinde mevcut olan spam ve spam olmayan e-postaların karakteristiklerine bakarak, gelecek dönemlerde ulaşan e-postaları, belirlediğimiz örüntü yardımı ile bulabilmek kolay olacaktır.

Gönderim tarihi: 29.11.2021 Kabul tarihi: 25.05.2022
DOI: 10.14514/BYK.m.26515393.2022.10/1.78-87

Bayes teoremi esasında bir olayı meydana getiren unsurlardan hangisinin daha etkili olduğunu belirleyen bir istatistiki modeldir. Sınıflandırma temeline dayanan bir model olması sebebi ile yapay zekâ algoritmaları ve Saldırı Tespit Sistemleri ile kullanılabilmektedir.

Farah Jemili tarafından DARPA 99 veri seti (DARPA 99 veri seti MIT Lincoln Laboratuvarı tarafından Saldırı Tespit Sistemlerinin verimliliğini ölçmek için tasarlanmış, farklı IP'ler arasındaki siber saldırı örneklerini içermektedir.) kullanılarak bir STS oluşturulmasında kullanılmış, bu çalışma ile %99,62 oranında DOS saldırılarının, %100 oranında bilgi tarama saldırılarının, %98,63 oranında U2R saldırılarının ve son olarak %42,62 oranında RL2 saldırılarının tespiti başarılı olmuştur (Jemili ve ark., 2007).

Dewan ise KDD CUP99 veri setini (KDD Cup 99 veri seti KDD-99 Beşinci Uluslararası Bilgi Keşfi ve Veri Madenciliği Konferansı ile düzenlenen Üçüncü Uluslararası Bilgi Keşfi ve Veri Madenciliği Araçları Yarışması için kullanılan veri setidir. Yarışma görevi, izinsiz girişler veya saldırılar olarak adlandırılan "kötü" bağlantılar ile "iyi" normal bağlantıları ayırt edebilen bir tahmine dayalı model olan bir ağ saldırı detektörü oluşturmaktı. Bu veri tabanı, bir askeri ağ ortamında simüle edilen çok çeşitli izinsiz girişleri içeren, denetlenecek standart bir veri kümesi içerir.) kullanmış %99,49 oranında DOS saldırısını, %99,72 oranında bilgi tarama saldırısını ve %99,47 oranında U2R saldırısını ve %99,35 R2L saldırısının saptanmasında başarı kazanılmıştır (Farid ve Rahman, 2010).

4.2. Destek Vektör Makinesi (DVM)

Vapnik tarafından 1998 yılında ortaya atılmış, istatistiki modelleme tekniklerinden regresyon kullanarak, verilerin öğrenme esnasında oluşturulan karakteristik davranışlarının tanımında ve analizinde kullanılmakta olup, analist yönlendirmeli bir yapay zekâ algoritması olarak adlandırılmaktadır.

DVM'de başlangıçta verilen bilinen, saptanmış, etiketlenmiş veri iki parçaya bölünmekte, her bir yeni gelen veri bu iki gruptan birine dahil edilmek üzere istatistiki bir model içerisine yerleştirilmektedir. Bu modellemede temel varsayım iki kategorinin içerisindeki verilerin kategorileri iyi temsil etmesi ve iki kategorinin birbirinden kesin sınırlar ile ayrılmasıdır.

Saldırı Tespit Sistemlerinde kullanılmak üzere 2010 yılında Yongli Zhang KDD CUP 99 veri setini kullanmış, [18] %99,32, oranında normal davranışların, %93,81 oranında DOS saldırılarının, %33,67, bilgi tarama saldırılarının, %39,31 oranında U2R saldırılarının ve son olarak %99,42 R2L saldırılarının tespitini doğru olarak gerçekleştirmişlerdir (Zhang ve Zhu, 2010).

4.3. Karar Ağaçları

Karar ağacı sınıflandırma amaçlı kullanılan bir yapay zekâ algoritması olup, bir kök, iç düğümler ve terminal düğümü adı verilen yaprak şeklinde unsurlardan oluşmaktadır. Karar ağacında temel mantık kök olarak adlandırılan ana başlangıç noktası vereceğimiz kararı, kararın alternatiflerini ise düğümler oluşturmaktadır. Karar ağaçları oluştururken en önemli nokta algoritmanın belirlenmesidir. Farklı algoritmalar farklı sınıflandırmalara sebep olacaktır. Karar ağaçları kullanılarak oluşturulan yapay zekâ algoritmaları kök ve düğümlerine göre farklı isimler almaktadır. ID3, C4.5 ve C5 yaygın olarak kullanılmaktadır.

Gönderim tarihi: 29.11.2021 Kabul tarihi: 25.05.2022
DOI: 10.14514/BYK.m.26515393.2022.10/1.78-87

Ammar Alazab, 2012 yılında KDD CUP 99 verisini bir Saldırı Tespit Sistemi ile birleştirmiş, ve böylece %97,2 oranında DOS saldırılarını, %99,6 oranında bilgi tarama saldırılarını, % 92,5 oranında U2R saldırılarını ve son olarak saldırılarında %99,7 oranında ve R2L saldırılarını doğru olarak tespit etmiştir (Alazab ve ark., 2012).

4.4. Yapay Sinir Ağları

İnsan beyni içerisindeki nöronlar emsal alınarak oluşturulmuş Yapay Sinir Ağları (YSA) sınıflandırmadaki başarısı sebebi ile Saldırı Tespit Sistemlerinde kullanılmaktadır. Yapay sinir ağı, üzerinde bulunan yapay sinir hücrelerine ağırlıklandırılmış değerler verilmesi ile oluşturulur. Veri setinin sisteme öğretilmesi ağırlıklandırmayı belirleyen ana unsurdur. Ağırlık değişiminin mevcut olmaması öğrenme işleminin devam etmediğini göstermektedir. En çok kullanılan algoritma tipi çok katmanlı -Multi Layer Perceptron MLP olup, fonksiyon oluşturma, kategorize etmede büyük kolaylık sağlamaktadır.

Guisong Liu, KDD Cup99 veri seti ile HPCANN (Hierarchical Principal Component Analysis Neural Networks) ile Saldırı Saptama Sistemi oluşturmuş, bu sistemin %100 oranında DOS saldırılarını %100 oranında bilgi tarama saldırılarını ve %97,2 oranında ise R2L saldırılarını başarı ile doğru olarak belirlediği görülmüştür (Liu ve ark., 2007).

Yukarıda bahsi geçen dört farklı yapay zekâ algoritması ile oluşturulmuş Saldırı Tespit Sistemlerinin karşılaştırılması aşağıdaki tabloda yer almaktadır.

Tablo 1. Saldırı Tespit Oranları

	DOS	Bilgi tarama	R2L	U2L
Bayes	99,62%	100,00%	99,35%	99,47%
DestekVektör Makinası	100,00%	100,00%	99,42%	100,00%
Karar Ağaçları	99,98%	99,66%	99,70%	92,50%
Yapay Sinir Ağları	100,00%	100,00%	99,98%	99,85%

Tablodan çıkarılacak sonuç; Yapay Sinir Ağları ve Destek Vektör Makinası'nın yüksek performans gösterdiği, buna karşın Bayes ve Karar Ağaçları yöntemlerinin diğer iki yönteme göre daha az performans gösterdiği görülmüştür. Yapay Zekâ Algoritmalarının Saldırı Tespit Sistemlerinde kullanılmasının uygun bir yöntem olduğu görülmüştür.

4.5. Uzman Sistemler

Uzman sistemler en eski ve sıklıkla kullanılan bir yapay zekâ algoritmasıdır. Uzman sistemlerin yapısına bakıldığında, uzman gözlem ve önerilerinin yer aldığı bir veri tabanı işlevi gördüğü tespit edilebilir. Buna ek olarak veri tabanında yer alan bilgiler ışığında yorumlama kabiliyeti ve bu sayede cevapları veri tabanında bulunmayan sorular için de bilgi kaynağı görevi görmektedir. Uzman sistem kabuğu adı verilen yorumlama makinesi ve boş bilgi tabanının birleşiminden oluşan ana bir unsura sahiptir. Bu sistem kabuğunun diğer uygulama ve yazılımlar ile uyumlu olması çalışma performansı için önemlidir. Uzman sistem çalışma prensibi, mevcut sistem kabuğunun seçilmesi ve içerisinde bulunan boş veri tabanının uzman bilgisi ile doldurulması aşamalarını kapsamaktadır.

Gönderim tarihi: 29.11.2021 Kabul tarihi: 25.05.2022
DOI: 10.14514/BYK.m.26515393.2022.10/1.78-87

Saldırı Tespit Sistemi olarak Uzman Sistemler kullanılmak istenir ise bu daha çok mevcut güvenlik unsurlarının planlanması için kullanılacak ve böylece mevcut kaynakların uygun dağıtılması gerçekleşebilecektir (Kivimaa ve ark., 2009).

4.6. Akıllı Ajanlar

Akıllı ajanlar, saldırı anında cevap verme, iletişim dilini anlayabilme, sonucunda bir davranış geliştirme sistemi kurabilen bir yapay zekâ yazılımıdır. Davranış geliştirme, anlayabilme özelliklerinden ötürü yazılım sistemlerindeki nesnelerden ayrılırlar (Tyugu, 2011). Igor Kotenko tarafından yapılan bir çalışmada önerilen yaklaşım, çok ajanlı bir yapay zekâ simülasyonuna dayanmaktadır. Bu yaklaşıma göre oluşturulacak Saldırı Tespit Sistemleri daha önceden belirlenmiş kriterlere göre hareket eden, davranış geliştirebilen ajanlar tarafından oluşturulacaktır. Bu simülasyonun içerisinde ayrık olay, internet protokollerinin paket düzeyindeki halleri bulunmaktadır. Bu çalışma sonucunda kullanılan ajanların DDOS saldırılarını tespit edebildikleri görülmüştür (Kotenko, A. Ulanov, 2007).

4.7. Arama Yöntemi

Arama yöntemi tüm yapay zekâ programlarında bulunan ve programın verimliliğini belirleyen temel bir fonksiyondur. Bir arama fonksiyonunun geliştirilebilmesi için ana etken yardımcı unsurların aramaile ilişkilendirilebilmesidir. Oyun yazılımlarında, dinamik yazılımların içerisinde gömülü olarak güvenlik problemlerinin çözümünde kullanılmaktadır. En önemli çeşitleri ise stokastik arama, Andor ağaçları, minimax, αβ arama, yöntemleri olarak gösterilebilir. Özellikle kullanılan αβ-arama algoritması bilgisayardaki satranç programlarındaki problemlerin çözümünde kullanılmaktadır (Şeker, 2020).

Siber savunma sistemlerinde kullanımını ise Kivimaa tarafından "ParetoOptimal Situation Analysis for Selection of Security Measures" makalesinde sunulmuştur. Bu çalışmaya göre; Bir kullanıcının ayrı bir dinamik programlama yöntemi kullanarak Pareto optimali hesaplamasına dayalı olarak güvenlik önlemlerini rasyonel bir şekilde seçmesini sağlar. Bu, yalnızca standartların öngördüğü katı kısıtlamaları kullanmak yerine, mevcut kaynakları hesaba katan rasyonel karşı önlemlerin seçilmesini sağlar (Ojamaa ve ark., 2008).

5. Sonuç ve Değerlendirme

Ağ ve bilgisayar sistemleri sadece iş ve haberleşme alanlarında değil, yaşam alanları, sağlık, ulaşım, üretim vb. alanlarının vazgeçilmez bir öznesi haline gelmiş, bu sebeple ağ ve bilgisayar sistemlerine yapılacak olan her türlü saldırının etkisi yalnızca saldırılan alana değil, bu ağlarla çevrilmiş tüm noktalara sirayet edecektir. Bu saikle, ağ ve bilgisayar sistemlerinin saldırılardan korunması için alınacak önlemler büyük bir çalışma sahası haline gelmiştir.

Günümüzde Saldırı Tespit Sistemlerinin ilk örnekleri olan güvenlik duvarları, virüs programları vb.nin kullanımı halen devam etmektedir.

Gönderim tarihi: 29.11.2021 Kabul tarihi: 25.05.2022
DOI: 10.14514/BYK.m.26515393.2022.10/1.78-87

Geleneksel saldırı saptama sistemlerinin hız, performans, kapsadığı alan, saldırının doğru ve zamanında tespit edilebilmesi vb. sebeplerle yeterince özellikle ileriki dönemlerde yeterince etkinlik gösteremeyeceği düşünülerek, yapay zeka gibi anlık kontrol sağlayabilen, saldırı tespitinin doğru algılama oranı yüksek, insan faktörünün etkin rol almadığı sistemlere geçişin yüksek olduğu görülmüş, yapay zekanın Saldırı Tespit Sistemleri'nde kullanımının ise makine öğrenmesi ve analist öğretici olarak iki farklı sistemle ile mümkün hale getirildiği, bu iki yapının en büyük farkının birinin yapay zekayı mevcut veriler ile beslerken diğerinin mevcut veriler arasında bağlantı kurarak, makine tarafından üretilmesi olduğu görülmüştür. Saldırı Tespit Sistemleri ile Bayes, Destek Vektör Makinası, Karar Ağaçları, Yapay Sinir Ağları, Uzman Sistemler, Akıllı Ajanlar ve Arama yöntemlerinin sıklıkla kullanıldığı görülmüştür.

Yapılan çalışmalarda yapay zekanın Saldırı Tespit Sistemlerinde kullanılması için DARPA 99 ve KDD Cup 99 verilerinin kullanıldığı, bu verilerin Beşinci Uluslararası Bilgi Keşfi ve Veri Madenciliği Konferansı ile düzenlenen Üçüncü Uluslararası Bilgi Keşfi ve Veri Madenciliği Araçları Yarışması için kullanıldığı görülmüş, bu veri seti üzerinde yapılan çalışmalar ile en çok verim alınan yapay zekâ tekniğinin Yapay Sinir Ağları ve Destek Vektör Makinası olduğu tespit edilmiştir. Teknolojinin gelişmesi ile birlikte bundan sonra tasarlanacak Saldırı Tespit Sistemlerinin mekanizmalarının yapay zeka tabanlı olacağı; yapay zeka ile yapılan çalışmalarda saldırıların doğru ve hızlı tespit edilmesi ile öngörülmektedir. Yapay zekanın her alanda olduğu gibi Saldırı Tespit Sistemlerinde de lokomotif güç olacağı, saldırı tespit edilmesinde hız, güven ve tarafsızlık anlamında iyileştirmeler getireceği şüphesizdir.

Kaynakça

Alazab, A., Hobbs, M., Abawajy, J., & Alazab, M. (2012). Using feature selection for intrusion detection system. In *2012 international symposium on communications and information technologies (ISCIT)* (pp. 296-301). IEEE.

Anonim (2020). *Cyber Security Technology*. https://securelist.com/cyberthreats-on lockdown/96988.

Arıcı, N., & Yıldız, E. (2010). Gerçek Zamanlı Bir Saldırı Tespit Sistemi Tasarımı Ve Gerçekleştirimi. *E-Journal of New World Sciences Academy Engineering Sciences*, *5*(2).

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *arXiv preprint arXiv:1502.03552*.

Farid, D. M., & Rahman, M. Z. (2010). Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm. *J. Comput.*, *5*(1), 23-31.

Frank, J. (1994). *Artificial Intelligence and Intrusion Detection: Current and Future Directions.*

Haq, N. F., Onik, A. R., Hridoy, M. A. K., Rafni, M., Shah, F. M., & Farid, D. M. (2015). Application of machine learning approaches in intrusion detection system: a survey. *IJARAI-International Journal of Advanced Research in Artificial Intelligence*, *4*(3), 9-18.

Jemili, F., Zaghdoud, M., & Ahmed, M. B. (2007, May). A framework for an adaptive intrusion detection system using Bayesian network. In *2007 IEEE Intelligence and Security Informatics* (pp. 66-70). IEEE.

Kivimaa, J., Ojamaa, A., & Tyugu, E. (2008, October). Graded security expert system. In *International Workshop on Critical Information Infrastructures Security* (pp. 279-286). Springer, Berlin, Heidelberg.

Gönderim tarihi: 29.11.2021 Kabul tarihi: 25.05.2022
DOI: 10.14514/BYK.m.26515393.2022.10/1.78-87

Kotenko, I., & Ulanov, A. (2007, June). Multi-agent framework for simulation of adaptive cooperative defense against internet attacks. In *International Workshop on Autonomous Intelligent Systems: Multi-Agents and Data Mining* (pp. 212-228). Springer, Berlin, Heidelberg.

Liu, G., Yi, Z., & Yang, S. (2007). A hierarchical intrusion detection model based on the PCA neural networks. *Neurocomputing*, *70*(7-9), 1561-1568.

Ojamaa, A., Tyugu, E., & Kivimaa, J. (2008). Pareto-optimal situaton analysis for selection of security measures. In *MILCOM 2008-2008 IEEE Military Communications Conference* (pp. 1-7). IEEE.

Şeker, E. (2020). Yapay Zeka Tekniklerinin/Uygulamalarının Siber Savunmada Kullanımı. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *6*(2), 108-115.

Tanrıkulu, H. (2009). Saldırı Tespit Sistemlerinde Yapay Sinir Ağlarının Kullanılması. (Doctoral dissertation, Yüksek Lisans Tezi, Ankara Üniversitesi Fen Bilimleri Enstitüsü, Ankara)

TUIK. (2021). *Hane halkı Bilişim Teknolojileri Kullanım Araştırması.* www.tuik.gov.tr

Tyugu, E. (2011, June). Artificial intelligence in cyber defense. In *2011 3rd International conference on cyber conflict* (pp. 1-11). IEEE.

Veeramachaneni, K., Arnaldo, I., Korrapati, V., Bassias, C., & Li, K. (2016, April). AI^ 2: training a big data machine to defend. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 49-54). IEEE.

Zhang, Y., & Zhu, Y. (2010, May). Application of improved support vector machines in intrusion detection. In *2010 2nd International Conference on E-business and Information System Security* (pp. 1-4). IEEE.