SALDIRI TESPİT SİSTEMLERİNDE YAPAY SİNİR AĞLARININ KULLANILMASI

Dr. Murat H. Sazli
Ankara Üniversitesi
Elektronik Mühendisliği Bölümü
sazli@eng.ankara.edu.tr

Haluk Tanrikulu
haluk@ieee.org

ÖZET

Bu çalışma ağ üzerinden yapılan saldırıları ve onlara karşı geliştirilen saldırı tespit mekanizmalarında (IDS, Intrusion Detection System) yapay sinir ağları kullanılmasına bir örnek oluşturulması ve incelenmesini içermektedir.

Yapay Sinir Ağları (YSA) kullanarak bir ağ üzerinde akan paketlerin hangi saldırı yöntemi kullandığının bulunması bu çalışmanın konusudur. Bu nedenle öncelikle saldırı tespit sistemlerinin ne şekilde yapılandıkları, hangi yöntemleri kullandıkları incelenmiştir. Ardından genel olarak saldırı tipleri ve özellikleri ele alınmıştır. Bu saldırılardan ağ da anormalik yaratan saldırılardan "Neptune" ve "the ping of death" 'ın bulunması için Çok Katmanlı Algılayıcı (Multi Layer Perceptron (MLP)) yapay sinir ağ modeli kullanılarak bir yapay sinir ağı oluşturulmuştur. Ağ kurulmasında MATLAB programı kullanılmıştır. Yapay sinir ağında kullanılacak veri setleri DARPA veri setlerini örnek alarak, bir kamu ağından toplanan ağ paketlerinden oluşturulmuştur. Oluşturulan veri setleri ile MATLAB programına uygulanmıştır.

Anahtar Kelimeler: saldırı tespit, yapay sinir ağları, çok katmanlı,

1. GİRİŞ

WWW (World Wide Web) ve yerel ağ sistemlerinin hızlı gelişimi ve yayılması son yıllarda bilgisayar ve bilgi iletişim dünyasını değiştirdi. Birbirlerine bağlanan bilgisayar sayılarının artması ile bilgisayar ve ağ sistemlerine izinsiz giriş yapmak isteyenler (intruders) ve ağ korsanlarına (hackers) yeni kapılar açtı. Bu tür açık kapılardan sızmalar ile sistemlere geçici veya kalıcı zararlar verildi. Bu nedenle şirketler, araştırma firmaları, organizasyonlar kendi ağ yapılarındaki veri akışınının güvenliğini sağlayacak yeni sistemler geliştirdiler. Bu sistemlere genel olarak saldırı tespit sistemleri (IDS, Intrusion Detection System) denilmektedir [1].

2. SALDIRI TESPİT SİSTEMLERİNİN (STS) YAPISI

Saldırı Tespit Sistemleri bir ağ veya bir bilgisayara karşı yapılan her türlü saldırının tespit edilmesi ve saldırının bertaraf edilmesi için geliştirilmiş sistemlerin bütününe denir.

Bir STS tasarımında iki ana yaklaşım vardır [2].

- **İmza Tanıma Temelli veya Kötüye Kullanım yolu ile saldırı tespiti** : Ağda kötü amaçlı kullanımların tespitidir. Bilinen sistem açıklarını ve saldırı imzalarının kullanılması ile oluşan eylemlerin araştırılması ile saldırıların tespit edilmesi olarak tanımlanabilir. Kötüye kullanım tespiti (Misuse detection) ya da imza-tanımaya dayalı sistemlerde her davranışın bir imzası-karakteri vardır. Bunlar daha önce görülen davranış şablonlarıdır.

Eğer gözlenlenen davranış daha önceden bilinen bir saldırı imzası ile eşleşiyorsa saldırı olarak sı-

nıflandırılır. Daha önce karşılaşılmadıysa saldırı olarak nitelenmez. Bu sistemler saldırıyı kesin olarak tanıyabilmesidir. Yani yanlış alarm vermezler fakat yeni bir saldırı gelirse bunu sezemezler [3].

Uzman sistemler çoğunlukla bu yaklaşımı kullanırlar. STS tasarımlarında kural tabanlı uzman sistemlerin oluşuturulmasında Denning 'e [4] ait olan profil modelini kullanılmaktadır. Bu modelde uzman sistemler eşik değeri, istatiksel momentum kullanımı veya Markov modelini kullanmaktadırlar.

- Ağ üzerinde oluşan anormal (abnormal) ağ traffiğinin incelenmesi ile saldırıların tespiti: Anormal ağ trafiği, ağ içerisinde meşru kullanıcıların kendi hak ve sınırlarını aşması veya diğer bağlantılarda oluşan ağ akışını engeleyecek kadar ve kabul edilebilecek sınırları aşan eylemlerin ortaya çıktığı ağ trafiğidir.

Kısaca ağda oluşan anormallikleri gözlemleyerek, saldıryı belirlemek mümkündür. Bu tip modellere ağ aktivitesi modelleri (Network activity models) adı verilir ve ağdaki trafik yoğunluğu üzerinden saldırı tespitine odaklanırlar. Bu saldırılar bilgi tarama (Probe) ve Hizmet Engelleme (Denial of Service – DoS) olarak bilinen saldırıların yakalanmasında kullanılmaktadır.

Normal bir sistemde kullanıcı istekleri tahmin edilebilir bir yapıdadır. Burada normal davranışın bilinmesi ve modelenmesi esastır. Ancak bundan sonra bir anormallik varsa tespit edilebilir. Normal davranış belirli kurallar ile tanımlanabilir ve bu tanımlar sınırları dışında kalan davranışlar anormallik olarak değerlendirilir ve sapmanın şiddetine göre saldırı olarak sınıflandırılabilir. Bu yöntemin avantajı daha önceden tanınmayan saldırıların keşfedilmesi olasılığıdır. Dezavantajı ise yanlış alarmların (false alarm/positive) sayısının yüksek olmasıdır [1].

Anormallik tespitinde istatistiksel yöntemler, yapay sinir ağları, veri madenciliği bilgisayar bağışıklık sistemi (computer immunology) gibi birçok yaklaşım uygulanabilir [5].

Çalışmamızda Çok Katmanlı Algılayıcılar (ÇKA - Multi Layer Perceptron (MLP) yapay sinir ağını (YSA) kullanarak bir saldırı tespit sisteminin ağ yapısını oluşturacağız. Daha önce yapılan çok sayıdaki çalışmalarda [6],[7],[8],[9] YSA kullanarak sisteme yapılan atakların normal veya saldırı nitelikli olduğu tespit edilmişken, buradaki çalışmamızda atağın tipinin belirlenmesine çalışılmıştır.

3. SALDIRI TİPLERİ VE ÖZELLİKLERİ

Ağ üzerinden yapılan saldırılar 4 temel kategoriye ayrılırlar. [3]

a) Bilgi Tarama (Probe ya da scan): Bu saldırılar bir sunucunun ya da herhangi makinanın, geçerli ip adreslerini, aktif giriş kapılarını (port) veya işletim sistemini öğrenmek için yapılırlar. [3]

Örneğin;

a. Belirli bir protu sürekli tarama saldırısı (ipsweep).

b. Bir sunucu üzerindeki hizmetleri bulmak için tüm portları tarar (Portsweep).

b) Hizmet Engelleme (Denial of Service - DoS): TCP/IP protokol yapısındaki açıklardan faydalanarak veya bir sunucuya çok sayıda istek yönelterek sunucunun iş göremez hale gelmesini sağlayan saldırılardır. DoS saldırıları kendi içinde gruplara ayrılır [10].

"The ping of death" (ölümüne ping) saldırısı protokol hatalarından faydalanarak yapılan bir saldırı şeklidir. Bu atakta bir tek büyük boyutlu

ICMP eko mesajı gönderilerek sistemin cevap verermemesi sağlanmış olur.

Şekil 1: DoS saldırı tipleri [3]

Başka bir saldırı şekli ise TCP SYN paketinin içerisine kaynak ve varış adresi aynı makine (bilgisayar) olan bir paket gönderilmesiyle olur. Bunlar tek paketle ya da az paketle gerçekleştirilen, protokollerin açıklarını kullanan saldırılardır [3]. Bu iki atak şekli ilerleyen konu başlıkları altında detaylı olarak anlatılacaktır.

Bir sunucudan sürekli istekte bulunulmasına dayanan saldırı yöntemi ile hem sunucu makineyi hem de ağı meşgul eder.

Benzer saldırı şekilleri aşağıda sıralanmıştır [3].

a. ICMP mesajlarının broadcast ile tüm ağa dağıtılmasıyla oluşur (Smurf).
b. Kullanıcının makinayı sürekli pinglemesiyle gerçekleşir (Selfping).
c. Saldırgan kurbanın kurmaya çalıştığı bağlantılar için kurban adına "reset" göndererek bağlantısını engeller (tcpreset).
d. Saldırgan sunucuya sürekli mail gönderir (mailbomb).

c) Yönetici Hesabı ile Yerel Oturum Açma (Remote to Local - R2L): Kullanıcı haklarına sahip olunmadığı durumda misafir ya da başka bir kullanıcı olarak izinsiz erişim yapılmasıdır [3]. Bunlara örnek:

a. Unix işletim sistemi üzerinde çalışan bir trojan saldırısıdır (Sshtrojan).

b. Tahmini kolay şifreleri bularak sisteme girilmesidir (guest).

d) Kullanıcı Hesabının Yönetici Hesabına Yükseltilmesi (User to root - U2R): Bu tip saldırılarda sisteme girme izni olan fakat yönetici olmayan bir kullanıcının yönetici izni gerektirecek işler yapmaya çalışmasıdır [3]. Bunlarda bazıları aşağıda sıralanmıştır.

a. Solaris üzerinde eject programı ile tampon taşmasına (buffer flow) yol açıp, yönetici haklarına sahip olunmasıdır (**Eject)**.

b. Sql veritabanı kurulu Linux makinalarda sunucuya bağlanan kullanıcının belirli komutlarla yönetici hakları ile komut satırı elde etmesidir (**Sqlattack)**.

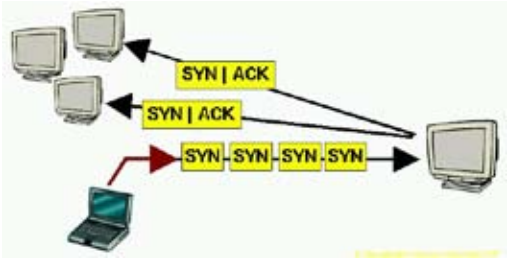
STS'ler saldırı tiplerine göre sınıflandırılmaktadır. 1. ve 2. tip saldırılar ağ tabanlı STS'ler ile engellenirken, 3. ve 4. saldırılar ise sunucu (host) tabanlı STS'ler ile engellenmektedir. Bizim çalışmamızda kurmayı planladığımız STS ağ tabanlı STS'dir.

Tespit Edilecek Saldırılar

Bu çalışmamızda DoS saldırılarından ikisini kullanacağız : "SYN Flooding (Neptune)" ve "The Ping of Death". Bunun nedeni iki saldırı şeklininde ağda bir anormallik aratması ve yapay sinir ağlarının bu anormalliği tespitindeki başarının görülmesini sağlamaktır. aşağıda bu iki saldırını kısa açıklamaları yer almaktadır.

SYN Flooding (Neptune) Saldırısı
Bilgisayar sistemi TCP/IP "stack" adı verilen bir bölgede tüm bağlantı bilgilerini tutar. TCP bağlantı temelli bir erişim sağladığı için üç yollu el sıkışma modelinin gerçekleşmesi gerekir. İki bilgisayar bağlantısında bağlantıyı talep eden ta-

raf karşı tarafa SYN paketi gönderir. Karşı taraf ise cevap olarak SYN/ACK paketi ile daveti kabul ettiğini belirten bir paket gönderir. Daha sonra ilk taleb eden tekrar ACK göndererek bağlantının kurulmasını sağlamış olur. TCP 'nin bu çalışma şekli istendiğinde kötü amaçlar için kullanılır. Bunu şöyle açıklayabiliriz. Bir kişi bir sunucuya SYN paketi gönderirken bu paketin özelliği içindeki "Source ip" kısmına paketi gönderen kişinin IP adresi yerine aslında gerçekte varolmayan bir IP adresi yazarak gönderir. Bu esnada sunucu bu "SYN" paketini alır ve bağlantı işleminin tamamlanması için varolmayan IP adresine "SYN+ACK" paketi gönderir. Sunucu "SYN+ACK" paketinin cevabını (ACK) varolmayan bu IP adresli makineden beklemeye başlar. Bu bekleme sırasında varolmayan bu IP adresi bilgisayarın "TCP/IP stack" 'inde tutulur. Doğal olarak varolmayan IP adresli makineden "ACK" paketi gelmez ve bir süre sonra sunucunun "TCP/IP stack" 'i taşar ve ağ işlemez hale gelir. Bu saldırı "SYN Flooding" olarak tanımlanıyor. Sunucunun "TCP/IP stack" alanının doldurulması ile sunucu etkisiz hale getirilir. Kısaca sunucu artık kendisine gelen SYN bağlantı kur davet paketlerine cevap veremez hale gelir [15].



Şekil 2: SYN Flooding Atağı [14].

"SYN Flooding" büyük bir ağda bir sunucuyu etkisiz kılıyorsa ağın genelinde oluşan paketlerin incelenmesi ile anlaşılması oldukça zordur. Buradaki çalışmamızda ağ içindeki sunucu ve bilgisayar sayısı oldukça çoktur. Bu nedenle saldırı yöntemi önce yapay sinir ağına öğretilir daha sonrada bu saldırıyı bulması istenir. SYN Flooding TCP protokolunün üç yollu el sıkışma modelinin kötüye kullanımından başka birşey değildir. Bu yüzden ağda "ACK" ve "SYN/ACK" paketlerini bulunması kolaylık sağlıyabilir. Ancak paketler kapalıdır ve içerikleri bilinmemektedir. Ancak bir ağ paket analiz programı (sniffer programı) ile anlaşılabilir. Ancak STS'ler her paketin içeriğine bakacak kadar hızlı olamadıkları için saldırının motifinin belirlenmesine çalışılması gerekir. Ayrıca "SYN Flooding" sadece paket analizi ile de anlaşılması güçtür. Çünkü kurban sistem (sunucu) saldırı esnasında dışarıya paket gönderebilirken, gelen çağrılara cevap veremez durumdadır.

"The Ping of Death" Saldırısı

ICMP protokolü ağda bilgisayarların hata mesajlarını birbirlerine göndermesini yada "Ping" gibi basit işlemlerin yapılmasını sağlar. ICMP spesifikasyonunda, ICMP "Echo request" 'lerin veri kısmı 216 ile 65,536 byte arasında olmak zorundadır. Eğer bu veri sınırlarının dışına taşmış bir paket sunucu sisteme yollanırsa işletim sistemi böyle bir şey beklemediği için çalışamaz duruma gelecektir [15].

"The Ping of Death" ile artık sistemler tarafından kolalıkla fark ediliyor. Çalışmamızda kullandığımız paket boylarını küçük tuttarak diğer paket boyları (http, ftp hizmetinde kullanılanlar) ile karışmasını ve yapay sinir ağının sadece paket boyuna bakarak değilde paket dağılım motifine göre karar vermesini sağlanmasına çalışılmıştır.

4. ÇOK KATMANLI ALGILAYICILAR (MULTİ LAYER PERCEPTRON (MLP))

Çok Katmanlı Algılayıcılar (ÇKA); günümüzde birçok probleminin çözümünde kullanılmaktadır. Bugün özellikle sınıflandırma işlemlerinde en çok kullanılan yöntemlerin başında gelmektedir. ÇKA' da Delta öğrenme kuralı denilen bir öğrenme yöntemini kullanılmaktadır. Bu kuralın amacı; ağın istenen çıktı ile ürettiği çıktı arasındaki hatayı minimum yapmaktır [19].

ÇKA'lar; girdi katmanı, gizli katmanlar ve çıktı katmanı olmak üzere 3 katmandan oluşmaktadır. Bilgiler girdi katmanından ağa tanıtılır, gizli katmanlardan çıktı katmanına ulaşır ve çıktı katmanından dış dünyaya aktarılır. ÇKA'larda; eğiticili öğrenme yöntemi kullanılmaktadır. Ağa hem örnekler, hem de bu örneklerden oluşturulması gereken çıktılar sunulmaktadır. Ağ; örneklere bakarak problem uzayında bir çözüm üretir, bu genellemeye bağlı olarak gelecek yeni örnekler için de çözüm üretebilmektedir [19].

ÇKA'nın performansında öğrenme oranı ve momentum parametreleri büyük önem taşımaktadır.

Öğrenme oranı küçük seçilirse öğrenme işlemi yavaş olacak, büyük seçilirse değişimler kararsız olacaktır. Aynı zamanda; ÇKA'lar yerel sonuçlara da takılabilmektedir. Bu nedenle, momentum terimi kullanılmakta ve ele alınan problem için ağın ürettiği çözümler kabul edilebilir düzeye çekilmektedir [12][19].

ÇKA yapay sinir ağının eğitimi için eğitim (training) veri setlerine ihtiyaç duyulmaktadır. Bu veri setlerinin yardımı ile yapay sinir ağı atak motiflerini öğrenecektir. Bu nedenle eğitimde kullanılacak eğitim veri setinin oluşturulmasında çok dikkatli olunmalıdır. Veri setinin gerçektende ilgili olayların motiflerini yansıtığından emin olmak gerekir. Eğitilmiş yapay sinir ağının gerçekten atakları yakalayıp yakalamadıkları test etmek için en az bir tane test veri setine ihtiyaç duyulmaktadır.

5. VERİ SETİNİN OLUŞTURULMASI VE ÖZELLİKLERİ

Yaptığımız çalışmada veri seti mevcut bir kamu ağında akan paket analizinden elde edilmiştir. Verilerin toplanma yöntemi MIT Lincoln Laboratory tarafından 1998 yılında yapılan DARPA çalışmasındaki yöntemin aynısıdır [13]. DARPA ağının detayları bir sonraki bölümde anlatılmaktadır.

Ağ içerisinde 1200 yakın bilgisayar, yazıcı, sunucu ve kablosuz erişim cihazı bulunmaktadır. Ağ içerisine ağ paketlerini toplaması için ağ (paket algılayıcı) analiz yazılımı olan Ethereal Network Protocol Analyzer [17] kullanılmıştır. Bu yazılım ile ağ üzerinden o an geçen trafikler her 10 dakikada bir 2 dakikalık süreler zarfında toplanmıştır. Ağ analiz programı (Ethereal Network Protocol Analyzer) ile toplanan trafik ağ protokolleri taşıdıkları protokollere göre gruplara ayrılmıştır. Trafikler ethernet, FDDI, FiberChanel, IPX, TCP, Token Ring, UDP, Wlan gibi paketlere göre tek tek toplanıp analiz edilebilmektedir.

Yukarıda tanımladığımız ve çalışmamızda tespit etmeyi düşündüğümüz saldırı yöntemleri ("Neptune" ve "the ping of death") sadece TCP protokolunu kullandığı için diğer trafikler göz önünde bulundurulmamıştır. Genel olarak toplanan veri setlerinde % 42 IP (%5 TCP, %36 UDP, %1 ICMP), % 40 ARP, % 7 IPX protokolünü kullanan paketlerden oluşmaktadır. Ethereal Network Protocol Analyzer programında yapılan bir filtreleme ile TCP paket trafiğini aşağıdaki başlıklara göre sıralanmıştır.

Tablodaki başlıkların açıklamaları aşağıda sıralanmıştır.

Address A **Talep Eden IP Adresi**
Address B **Talebe Cevap Veren IP Adresi**
Packets **Paket Sayısı**
Bytes **Paket Boyu**
Packet Type **Paket Tipi**

Daha sonra ağa dışarıdan "Neptune" ve "the ping of death" atakları uygulanmıştır. Atakların oluşturdukları trafik verileri Ethereal programı ile toplanmıştır. Bu atakların oluşturdukları anormal trafik DARPA test sonuçlarındaki atak motiflerine benzemektedir. Bu motifler daha sonra eğitim seti olarak kullanılacak veri seti içerisine yerleştirilmiştir. Saldırının tipini belirtmek için veri setlerindeki her bağlantıya bir değer atamamız gerekmektedir. Her bağlantıdaki

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Packet Type
212.155.11.105	1090	208.53.143.90	80	1	60	0	0	1	60	1
212.155.11.96	1993	212.175.70.49	631	1	62	1	62	0	0	1
212.155.11.82	1311	207.68.178.16	80	1	62	0	0	1	62	1
212.155.11.71	1142	64.4.60.7	80	1	60	0	0	1	60	1
212.155.11.71	1144	65.54.183.193	80	1	60	0	0	1	60	1
212.155.11.10	3249	83.66.160.20	80	2	120	0	0	2	120	1
212.155.11.10	3316	66.226.72.50	80	2	120	0	0	2	120	1
212.155.11.10	3244	83.66.160.21	80	1	60	0	0	1	60	1
212.155.11.10	3241	66.249.91.104	80	2	120	0	0	2	120	1
212.155.11.10	3375	84.44.114.44	80	1	62	0	0	1	62	1
212.155.11.10	3392	212.156.13.147	80	1	62	0	0	1	62	1
212.155.11.10	3396	212.156.13.147	80	3	706	0	0	3	706	1
212.155.11.10	3405	212.156.13.147	80	1	62	0	0	1	62	1
212.155.11.10	3412	212.156.13.147	80	1	62	0	0	1	62	1
212.155.11.10	3381	66.249.91.104	80	2	120	0	0	2	120	1

Tablo 1 : Veri İçerikleri ve Başlıkları

son sütün değerleri 0,1,2 değerlerinden birini almaktadır. Eğer eğitim setindeki bir bağlantı normal bir bağlantı motifini gösteriyor ise 0, " SYN Flooding - Neptune" atağını gösteriyor ise 1, "the ping of death" atağını gösteriyor ise 2 değeri almaktadır. Veri setinin text modundaki bir gösterimi aşağıda gösterilmiştir. Burada "Address A" ve "Address B" verilerinin çıkarılmıştır. Çünkü atak türünü öğrenmek için sürekli değişen IP adreslerini kullanmaya gerek yoktur. Her satır bir bağlantıyı göstermektedir.

139,139,1,243,1,243,0,0,2,0
1090,80,1,60,0,0,1,60,1,0
1993,631,1,62,1,62,0,0,1,0
1311,80,1,62,0,0,1,62,1,0
1142,80,1,60,0,0,1,60,1,0
1144,80,1,60,0,0,1,60,1,0
3249,80,2,120,0,0,2,120,1,0
....
....
1245,80,3,120,0,0,2,120,1,1
1247,80,2,182,0,0,3,182,1,1
1251,80,3,182 ,0,0,3,182,1,0
1261,80,3,3709,0,0,3, 3709,1,1
1263,80,2,120,0,0,2,120,1,1

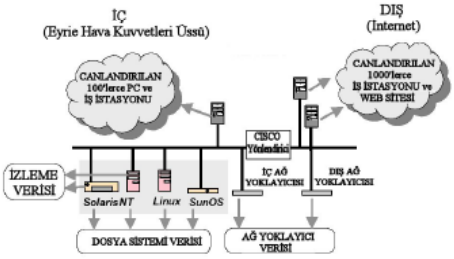
Paket tiplerine tcp=1, udp=2 ve icmp=0 olarak atanmıştır.

Yapay sinir ağlarında yukarıda oluşturulan veri seti girdi olarak ele alınmıştır. 270 adet örnek bağlantı 9 sütünda tanımlanmıştır. Böylece

270*9'luk bir matris oluşturulmuştur. Eğitim ve test setlerideki bu bağlantıların saldırı olduğunu göstermesi için bir de çıktı seti oluşturulmuştur. Bu veri seti 270*1'lık bir matristir.

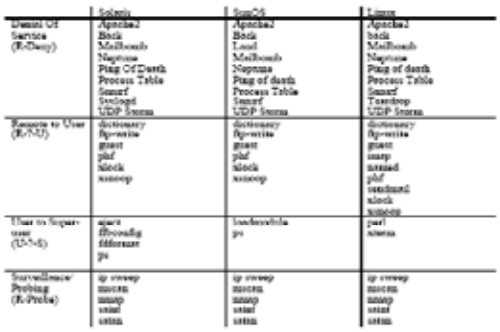
6. DARPA VERİ SETİ

DARPA'nın sponsorluğunda MIT Lincoln Laboratuarlarında STS'ler için bir karşılaştırma ortamı sunan IDEVAL veri setlerini oluşturulmuştur [13]. Saldırı tespit sistemlerinin sınanması amacı ile iki ağ kurulmuştur. Bunlar saldırıların hedefi olacak bir ağ ve saldırıları gerçekleştiren başka bir ağ olarak dizayn edilmiştir. İç ağda Amerikan Hava Kuvvetlerindeki bir yerel ağın simülasyonu gerçeklenmiştir. 1999 değerlendirmesinde kullanılan ağ aşağıdaki gibidir [3].



Şekil 3: DARPA ağının yapısı [3]

M.Erol'un çalışmasında [3] belirttiği gibi hava kuvvetlerini temsil eden ağ içerisinde dört "kurban" makine bulunmaktadır. Bunların üzerinde SunOS, Solaris, Linux, ve Windows NT işletim sistemleri bulunmaktadır. Şekilde görülen trafik oluşturucular yüzlerce sunucuyu ve çeşitli uygulamaları çalıştıran Internet kullanıcılarını simüle etmektedir. Protokollerin (HTTP, SMTP, telnet,...) karışımı, trafik yoğunluğunun saatlik degişimleri, 1998'de gerçek Hava Kuvvetleri agından toplanan trafiğe benzer olacak şekilde tasarlanmıştır. Ağ üzerinden 2 noktadan veri toplanmıştır: dört kurban makine ile yönlendirici arasındaki iç ağ dinleyicisi ve yönlendirici ile Internet arasındaki dış ağ dinleyicisi üzerinden [16].

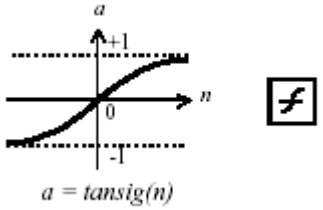


Şekil 4: DARPA 'daki ataklar [14]

7. ÇKA YAPAY SİNİR AĞININ OLUŞTURULMASI

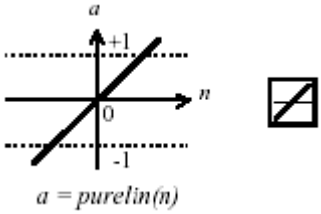
Yapay sinir ağları "MATLAB Neural Network Tools Box" 'ı kullanılarak EK-1'de belirtilen kodlar ile oluşturulmuştur.

Tüm uygulamalarda birinci katmanda "Tan-Sigmoid Transfer Fonksiyonu" (tansig(n)) kullanılmıştır. ÇKA uygulamalarında saklı katmanların tümünde Tan-Sigmoid Transfer Fonksiyonu kullanılmıştır. Bu fonksiyon grafiğinden de anlaşılacağı gibi yumuşak bir geçiş sağlamaktır [18].



Şekil 5 : Tansig(n) foksiyonu

Tüm uygulamalarda çıkış katmanında ise "Linear Transfer Function" (purelin(n)) kullanılmıştır. Bu fonksiyon ise keskin bir geçiş sağlamaktadır.



Şekil 6 : purelin(n) fonksiyonu

Öğrenme algoritması için "Levenberg – Marquardt" algoritmasının kullanıldığı trainlm kullanılmıştır. Bu algoritma çok fazla hafıza kullanmakla birlikte daha kısa sürede daha az epoch (devir) ile sonuça ulaşmaktadır.

Uygulamaların Geliştirilmesi

Tek katmalı uygulamalarda ara katman da 10 ve 20 nöron kullanılmış, çıkış katmanında da tek nöron kullanılmıştır. Çıkış değeri saldırı tipini belirlemektedir. Tek katmanda [10 1] ve [20 1] nöronla uygulama yapılmış, ancak başarım sağlanamamıştır.

Çok katmalı uygulamalarda saklı katmanlarda [10 10 1], [10 20 1], [10 30 1] olmak üzere üç deneme yapılmıştır. [10 10 1] nöronlu uygulamada "underfitting" özellikleri gözlenirken [10 20 1] nöronlu uygulamalarda başarım sağlanmıştır. [10 30 1] nöronlu uygulamalarda hedef değerine (goal) ulaşılmasına rağmen başarım sağlanamamıştır. 2. ara katman 40 nörona ([10 40 1]) çıkarıldığında "overfitting" görülmüştür.

Çok katmanlı uygulamalarda saklı katman sayısı artırılmasına rağmen başarım sağlanamamıştır.

En iyi başarım [10 20 1] nöronla kurulmuş yapay sinir ağı ile alınmıştır.

Öğrenme başarısı ve testler ile ilgili grafikler Ek-2'de verilmiştir.

8. TARTIŞMA

Bir ağda oluşan anormal veri akışlarının izlenmesinde YSA'nın kullanılması giderek yaygınlaşmaktadır. Bu yönde çok sayıda çalışma ticari ürün olarak karşımıza çıkmaktadır. Bu çalışmamızda yapay sinir ağlarının STS olarak kullanılmasındaki başarısı gözlenmiştir. Uzman sistemler, yapay zeka uygulamaları, istatistiki analiz metodları STS uygulamalarında alternatif çözümler olarak görülmektedir. Ancak iyi motiflenmiş bir veri seti ile YSA'nın başarısı %100 oranındadır. Ayrıca Ek-2'deki grafiklerde de görüleceği gibi minimum değerlerde oluşan anormal trafik değişimlerinide tespit etmekte başarılıdır.

9. SONUÇLAR

Bu çalışmada, çok katmanlı yapay sinir ağları ile internetten gelebilecek DoS ataklarının algılanması başarı ile sağlanmıştır. STS oluşturulmasında anormal trafiklerin dağılımına bakarak saldırının tipinin belirlenebileceği gösterilmiştir.

Başarımı en yüksek ağın [10 20 1] nöron sayılarına sahip çok katmanlı algılayıcı yapay sinir ağı olduğu görülmüştür. Yapılan test çalışmalarında verilen her saldırı kurduğumuz yapay sinir ağı aracılığı ile kolaylıkla tespit edilmiştir. Eğitim veri setinin oluşturulmasında DARPA veri setlerinin motifleri ile kendi yerel alan ağımızdan elde edilen verilerin kullanılması, test veri setinin tamamen gerçek ortamdan elde edilen verilerden oluşması çalışmanın gerçek trafiklerin incelenmesinde de kullanılabileceğini göstermiştir.

Yapılan çalışmada sadece DoS ataklarının motifleri kullanılmış olmasına rağmen DARPA veri setinden çıkarılan 38 atak motifinin de yapay sinir ağına öğretilmesi ile tüm saldırıların tiplerinin öğrenileceği görülmüştür [13].

KAYNAKLAR

[1] R. Kemmerer and G. Vigna, "Intrusion detection : a brief history and overview" Computer, vol. 35, no. 4, pp. 27 – 30, 2002.

[2] M. Moradi and Mohammad Zulkernine, "A Neural Network Based System for Intrusion Detection and Classification of Attacks" , Natural Sciences and Eng. Research Council of Canada (NSERC) Reports, 148-04, 2004.

[3] M. Erol, "Saldırı Tespit Sistemlerinde İstatistiksel Anormallik Belirleme Kullanımı", ITÜ, 2005.

[4] D. Denning, "An Intrusion-Detection Model", IEEE Trans on Software Enginering, vol. 13, no. 2, 1987.

[5] N. Wu, J. Zhang, "Factor Analysis Based Anomaly Detection", Proc. IEEE Workshop on Information Assurance, 2003.

[6] James Cannady, "Artificial neural networks for misuse detection," Proceedings of the 1998 National Information Systems Security Conference (NISSC'98), Arlington, VA, 1998.

[7] J. Ryan, M. Lin, and R. Miikkulainen, "Intrusion Detection with Neural Networks" AI Approaches to Fraud Detection and Risk Management: Papers from the 1997 AAAI Workshop, Providence, RI, pp. 72-79, 1997.

[8] Lília de Sá Silva, Adriana C. Ferrari dos Santos, José Demisio S. da Silva, Antonio Montes "A Neural Network Application for Attack Detection in Computer Networks", Instituto Nacional de Pesquisas Espaciais – INPE, 2002.

[9] S. Mukkamala, "Intrusion detection using neural networks and support vector machine," Proceedings of the 2002 IEEE International Honolulu, HI, 2002.

[10] A. Hussain, J. Heidemann, C. Papadopoulos, "Distingushing between Singnal and Multisource Attacks Using Signal Processing", Computer Networks, vol. 46, 2004.

[11] Ryu, J., Sung-Bae, C., "Gene expression classification using optimal feature/classifier ensemble with negative correlation" Proceedings of the International Joint Conference on Neural Networks (IJCNN'02), Honolulu, Hawaii , sayfa 198-203, ISBN 0-7803-7279-4, 2002.

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

[13] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, K. Das, "Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation", MIT Lincoln Laboratory Technical Report TR-1062, 2001.

[14] K. Graves, "CEH, Offical Certified Ethical Hacker Review Guide", Wiley Publishing, 2007.

[15] Osman Atabey ; http://www.tcpsecurity.com/doc/genel/temelsaldiriteknikleri.html

[16] M. A. Aydın, "Bilgisayar Aglarında Saldırı Tespiti için İstatistiksel Yöntem Kullanılması", ITÜ Yüksek Lisans Tezi, 2005.

[17] http://www.ethereal.com

[18] Howord Demuth, Mark Beale, Version 3, "Neural Network Toolbox For use with Matlab", 1998.

[19] Ç. Çatal, L. Özyılmaz, Analysis of Multiple Myeloma Gene Expression Data by Multilayer Perceptron