Saldırı Tespit Sistemleri Üzerine Bir İnceleme

Esra N. GÜVEN, Şeref SAĞIROĞLU

***Özet*—Bu çalışmada, Saldırı Tespit Sistemleri (STS) hakkında literatür araştırması yapılarak, bilgi ve bilgisayar güvenliği açısından önemi değerlendirilmiştir. Araştırma sonucunda elde edilen bilgiler doğrultusunda STS'lerin sınıflandırılmasında kulllanılan genel kriterlere ve STS'lerin geliştirilmesi için kullanılan klasik ve zeki yöntemler araştırılmıştır. STS'de kullanılan zeki yöntemlerden günümüzde en çok dikkat çekenlerden biri olan Yapay Sinir Ağlarının (YSA) STS'lerde kullanılmasının üstünlükleri gözden geçirilmiş ve STS'ler genel olarak değerlendirilmiştir.**

***Anahtar Kelimeler*—Saldırı tespiti, saldırı tespit sistemleri (STS), zeki STS, yapay sinir ağı.**

***Abstract*—In this paper, intrusion detection systems (IDSs) which are important tools for providing information and computer security were analyzed, the methods used in developing IDSs were reviewed, the studies on classical and intelligent IDSs were revised. Artificial neural networks, one of the intelligent techniques, used in IDS design were also summarized. IDSs were finally evaluated in general.**

***Keywords*—IDS, Intrusion Detection Systems, intelligent IDS, artificial neural network.**

I. GİRİŞ

BİLGİ çağını yaşadığımız şu günlerde, e-devlet, e-imza, e-ticaret gibi kavramlardan oldukça sık bahsedilmektedir. Gerek hız ve verimlilik artışı, gerekse kolaylık sağlaması nedeniyle birçok bilgi elektronik ortamlara aktarılmıştır. Ancak, kişisel veya kurumsal açıdan önemli bir bilginin, başkalarının eline geçmesi ile maddi ve manevi zararlara yol açabileceği görülmüştür. Geliştirilen e-devlet, e-kurum gibi projelerde güvenliğin en üst düzeyde tutulması ulusal bir amaç haline gelmiş, bu konuda hukuki ve teknolojik önlemler geliştirilmiştir [1].

Teknolojik önlemlerin geliştirilmesi sırasında bir varlık olarak bilgiyi, tehdit ve saldırılara karşı korumak için güvenlik duvarları, antivirüs yazılımları, saldırı tespit sistemleri (STS), saldırı engelleme sistemleri (SES) gibi araçlar geliştirilmiştir. Bu araçların belirlenen kural ve politikalara göre yapılandırılması, bilgi güvenliğimizi büyük ölçüde sağlayacaktır.

Günümüzde bilgi ve bilgisayar güvenliğinin öneminin kavranmasıyla, geliştirilen araçlardan biri olan Saldırı Tespit Sistemleri (STS), saldırılara karşı sistemimizde "alarm" niteliği taşıyan yazılım ve donanımlardır. STS'lerin kullanılması ile sistemlere yapılan yetkisiz erişimler ve kötüye kullanımlar tespit edilerek, bunların yol açabileceği zararlar engellenmiş olur. Bilgisayar sistemlerinde STS'lerin kullanılması ile birlikte, sisteme ne tür saldırıların daha çok yapıldığı, sistemdeki mevcut açıklar ve saldırganlar hakkında daha detaylı bilgiler elde edilebilir.

Esra N. GÜVEN is now PhD Student in Boston, USA e-mail: enguven8@hotmail.com
Şeref SAĞIROĞLU is now with the Department of Computer Engineering, Gazi University, Ankara, TURKEY (e-mail: ss@gazi.edu.tr).

II. SALDIRI TESPİT SİSTEMLERİ

Saldırı tespiti kavramı ilk olarak Anderson'un "Bilgisayar Güvenliği Tehdit Gözetleme ve İzleme (Computer Security Threat Monitoring and Survaillance)" makalesi ile 1980'de ortaya atılmıştır [9]. Bu çalışma, STS'lerin tanımlanması ve tanınması açısından büyük bir öneme sahiptir.

İlk nesil STS'ler, basit bilgisayar sistemleri üzerine düşünülmüştür. İkinci neslinde ise günümüzde STS'lerin vazgeçilmezi olan "denetleme izi (audit trail)" kavramı ve veritabanı mantığının bilgi güvenliği alanındaki önemi ortaya çıkmıştır. Bunu izleyen çalışmalarda, güvenlik konusundaki çalışmalara yardımcı olmak amacıyla günlük denetleme verilerinin otomatik araçlar ile elde edilmesi konusunda çalışmalar yapılmıştır [10]. 1985'ten itibaren bu akımla geliştirilen projelerde denetleme verileri üzerinde özenle durulmuş ve istatistiksel yaklaşımlar temel alınarak saldırı tespit modelleri geliştirilmiştir. Bu çalışmalardan biri olan IDES (intrusion detection expert system), Denning tarafından geliştirilmeye başlanan ve 1988-1992 yılları arasında yapılan çalışmaların birçoğunu üzerinde barındıran bir sistemdir [8]. Daha sonra ismi NIDES (next-generation intrusion detection systems) olarak değişen bu sistem, ikinci nesil saldırı tespit sistemlerinin en eski ve en bilinen çalışmalarından biridir. IDES, saldırı senaryolarının kural kümelerinin çıkarılmasıyla dizayn edilmeye başlanan kural tabanlı bir STS'dir. Denning çalışmasında 3 farklı istatistiksel model tanımlamıştır. Bu modeler [2];

- kullanıcının belirli aralıklarla bir işlemi tekrar etmesine izin veren ve eşik değerine göre anormallik olduğunu tespit eden model,
- istatistiksel momentlerin bilindiği varsayılarak tespit edilen sapmalar ile anormallik olduğunu tespit eden model ve
- anormalliklerin tek olaya değil bir diziye bağlı olduğu Markov modeliolarak verilmektedir.

STS'lerin geliştirilmesinde günümüze kadar istatistiksel yöntemlerin dışında, kural tabanlı (rule based), eşik değeri belirleme (threshold value), durum geçiş diyagramları (state transition diagrams), yapay sinir ağları (artificial neural

networks), veri madenciliği (data mining), yapay bağışıklık sistemi (artificial immune system), bulanık mantık (fuzzy logic) gibi farklı birçok yaklaşım uygulanmıştır [11, 12].

STS'ler, bilgisayarlar ve veri ağları için yeni bir güvenlik yaklaşımı sunmaktadırlar. Daha önce de belirtildiği gibi STS'lerin amacı, saldırı, yetkisiz kullanım, suistimal, sistem içi ve dışından davetsiz misafirlerin sisteme zarar vermesi gibi durumların teşhis edilmesidir. Saldırı tespit problemi, bilgisayar ağlarının hızlı şekilde artması ve bu artışın sonucu olarak sisteme erişiminin çoğalması ile davetsiz misafirlerin kimliklendirmeyi kolaylıkla reddetmesinden sonra büyük önem kazanmıştır [3].

STS'ler günümüze kadar farklı birçok kritere göre sınıflandırılmıştır. Bunlardan en çok bilinen sınıflandırma türü saldırı tespit yöntemine göre olup, anormallik tespiti ve kötüye kullanım tespiti olarak ikiye ayrılır [8]. Ancak STS'lerin mimari yapısı, korunan sistemin türü, verinin işlenme zamanı gibi farklı sınıflandırmalar da yapılabilir [6]. Bu sınıflandırma kriterlerinden en yaygın olanları şunlardır;

Veri İşleme Zamanı

STS'ler için veri işleme zamanı, izlenen olaylar ve olayların analizi arasında geçen zamanı ifade eder. STS'ler "gerçek zamanlı" ve "gerçek zamanlı olmayan" şeklinde ikiye ayrılırlar [6].

Mimari Yapı

STS'lerin mimari yapısı, fonksiyonel bileşenlerin birbirlerine göre nasıl yerleştirildiklerini anlatır [13]. Temel fonksiyonel bileşenler; izlenen sistem, analizin yapıldığı sunucu ile çevresi ve problemler için izlenen hedef olarak sıralanabilir.

Bilgi Kaynağı

STS'ler, bilgi kaynaklarını analiz ve karşılaştırma yapmak için kullanırlar. Bilgi kaynakları, bilgisayar veya ağ paketlerinin dinlenmesinden elde edilebildiği gibi, kullanıcı profillerinin davranış modellerinden de elde edilebilir. Bilginin nasıl ve nereden toplanacağı, geliştirilecek olan STS'nin amaçlarına göre değişir. Bunlar; denetleme izi, ağ paketleri, uygulama kayıt dosyalarıdır.

Saldırı Tespit Yöntemi

STS'lerde, saldırı tespit yöntemi olarak anormallik tespiti ve kötüye kullanım tespiti olmak üzere iki farklı yaklaşım kullanılır [8]. Anormallik tespitine dayanan yaklaşım, sistemdeki kullanıcı davranışlarını modellerken, kötüye kullanım (imza) tespitine dayanan yaklaşım, saldırganların davranışlarını modeller.

Korunan Sistem

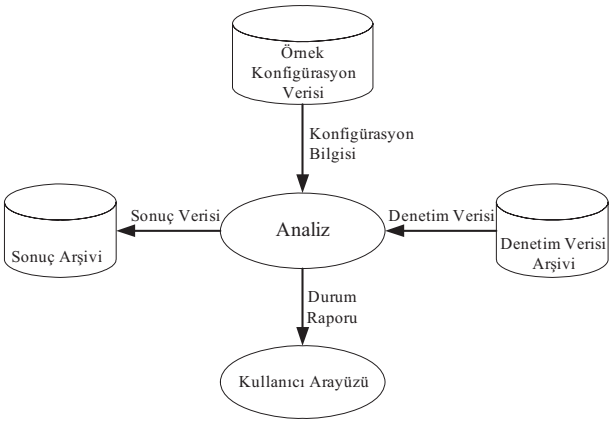
STS'ler korudukları sisteme göre üç gruba ayrılırlar. Korumak istenen sisteme göre; ağ, sunucu ya da uygulama temelli STS'ler olarak adlandırılırlar [14].

En genel anlamıyla, saldırı tespiti işini yapmak için geliştirilen sistemlere "saldırı tespit sistemleri" denir. Ancak günümüze kadar yapılan araştırmalar ve çalışmalar incelendiğinde, saldırı tespit sistemlerinin farklı tanımları olduğu görülmüştür. Yapılan bu tanımlara göre STS'ler;

- Bilgisayar sistemlerine yapılan atakları ve kötüye kullanımları belirlemek için tasarlanmış sistemlerdir [2].
- Tercihen gerçek zamanlı olarak, bilgisayar sistemlerinin yetkisiz ve kötüye kullanımı ve suistimalini tespit etmek için kullanılırlar [3].
- Saldırıyı durdurma girişiminde bulunmayan ve olası güvenlik ihlali durumlarında, sistem güvenlik çalışanlarına uyarı mesajı (alarm) veren sistemlerdir [4].
- Bilgisayar sistemlerinin kaynaklarına veya verilerine yetkisiz erişimleri belirler [5].
- Bilgisayar güvenliği alanındaki "hırsız alarm"larıdır [6].
- Bilgisayar veya ağ sistemine yapılan yetkisiz erişimleri tespit etmek için kullanılan yazılım araçlarıdır. STS'ler kötü niyetli ağ trafiği ve bilgisayar kullanımını tespit etme yeteneğine sahiptir. Bir STS, olası güvenlik açıklarını belirleyebilmek için bilgisayar veya ağ içerisinde değişik alanlardan bilgileri toplar ve analiz eder. Güvenlik duvarının statik izleme kabiliyetini tamamlayan dinamik izleme elemanıdır [7].

Yukarıda sunulan tanımlardan yola çıkarak, biz de STS'leri, bilginin elektronik ortamlarda taşınırken, işlenirken veya depolanırken başına gelebilecek tehdit ve tehlikelerin ortadan kaldırılması amacıyla, bilgiye yetkisiz erişim veya kötüye kullanım gibi girişimleri tespit edebilme ve bu tespiti sistem güvenliğinden sorumlu kişilere iletebilme özelliğine sahip yazılımsal ve/veya donanımsal güvenlik araçları olarak tanımlayabiliriz. Aynı zamanda STS'ler, ağ cihazlarını izleyerek anormal davranışları ve kötüye kullanımı tespit ederler.

Literatürdeki STS çalışmaları incelendiğinde, STS'lerin yapısı ile ilgili birçok gösterim yapıldığı görülmüştür. STS çalışmalarından biri olan NIDES'in geliştirilmesi sırasında çizilen örnek Şekil 1'de gösterilmiştir [8].



Şekil 1. STS'lerin temel yapısı [8]

Şekil 1'de sunucu tabanlı bir STS'nin temel yapısına bir örnek gösterilmiştir. Bu örnekte, bilgi kaynağı olarak denetim verileri kullanılmıştır. Denetim verisi arşivinden alınan denetim verileri, örnek konfigürasyon verileri ile karşılaştırılıp analiz edilerek, elde edilen sonuçlar, sonuç arşivine aktarılmaktadır. Aynı zamanda, olası saldırıların, kullanıcı tarafından görülebilmesi için kullanıcı arayüzüne de analiz sonuçlarını içeren durum raporu gönderilmektedir. İstenildiği takdirde, sonuç arşivi incelenebilir veya örnek konfigürasyon verileri güncellenebilir [8].

III. STS'LERDE KULLANILAN TEKNİKLER

Günümüze kadar STS'lerde birçok farklı teknik kullanılmıştır. Bu teknikler, elde edilen verilerin modellenmesi, sınıflandırılması veya kural tablolarının oluşturulması için geliştirilmiştir. Kullanılan tekniklerden elde edilen veriler sayesinde, saldırı tespit yaklaşımlarının uygulanması için gerekli olan platform oluşturulmuştur. Bu tekniklerden en çok kullanılanları, veri madenciliği, kural tabanlı sistemler, açıklayıcı istatikler, eşik değeri tespiti, durum geçiş analizi, uzman sistemler, örüntü eşleme olmuştur.

Veri Madenciliği

Veritabanındaki saklı olayları ortaya çıkarmak için yapılan bilgi açılımıdır. Paternleri ve veriler arasındaki ilişkileri bularak kural çıkarmak için kullanılır. Bu şekilde, hesap izlerini kullanarak normal kullanıcı aktiviteleri tanımlanır [15].

Kural Tabanlı (Rule Based) Sistemler

Sistem trafiğini inceleyip kurallar oluşturur ve saldırı tespiti sırasında belirlenen kurallara göre davranışlar sınıflandırılır [16].

Açıklayıcı İstatistikler (Descriptive Statistics)

Kullanıcı veya sistem davranışları farklı değişkenlere göre ölçülerek istatistiksel bir model oluşturulur. Bu değişkenlerden bazıları; kullanıcı oturum girişi, oturum kapatma, belli bir zaman periyodunda erişilen dosya sayısı, kullanılan disk alanı ve hafıza olarak sıralanabilir. Kullanıcı profilleri ve hesap izleri kullanılarak normal davranışların modeli oluşturulur ve anormallik tespit edilir [17]. Kullanıcı profilinin basit istatistiklerle oluşturulup, buradan uzaklık vektörlerini (distance vector) kullanarak karar alan sistemlerdir. Davranış profili oluşturulurken, kullanılan işlemci zamanı, bir zaman periyodundaki ağ bağlantı sayısı gibi farklı ölçütler de kullanılabilir. İstatistiksel yaklaşımların dezavantajlarından biri, saldırganın bu istatistikleri öğrenerek ona göre davranış sergileyebilmesidir [18].

Eşik Değeri Tespiti

Bu model oluşturulurken spesifik olayların tekrarlama sayısı ve spesifik zaman periyodu dikkate alınır. Karşılaşılan en büyük sorun; eşik değerinin belirlenmesi ve spesifik olaylar için pencere boyutunun belirlenmesidir. Örnek olarak; yanlış girişler, giriş/çıkış hata sayısı veya silme sayıları verilebilir. Tek başına pek güçlü değilse de büyük STS'lerde alt bileşen olarak kullanılır.

Durum Geçiş Analizi

Durum değişimi serileri oluşturularak gerçekleştirilir. Bir işin yapılması için birbirini takip eden durum sırası olduğu varsayılır ve buna göre bir seri oluşturulur. Sızmaların senaryosu çıkarıldıktan sonra, anahtar hareketler, imza hareketler olarak tanımlanır. İmza hareketler, saldırının tamamlanması için gereken en küçük hareket kümesidir. Durumlar, geçişler ve imzalar, durum geçiş diyagramı olarak grafiksel biçimde sunulur [19]. Burada tüm davranışlar durumlara karşı düşer. Eğer bir davranış daha önceden tanımlı durumlara ve durum geçişlerine denk düşen hareketler yapıyorsa saldırı olarak tanınır.

Uzman Sistemler

Belirli bir alanda sadece o alan ile ilgili bilgilerle donatılmış ve problemlere o alanda uzman bir kişinin getirdiği şekilde çözümler getirebilen bilgisayar programları olarak tarif edilebilir. Saldırı tespit sistemlerinin ilkleri kural-tabanlı uzman sistemlerdir [6].

Örüntü Eşleme

Sistemde daha önceden karşılaşılmaması gereken durumların tanımlanarak, bu durumlardan biri ile eşleşilmesi halinde saldırı olduğunu algılamak amacı ile kullanılır. Yapısı itibariyle esnek birçözüm değildir fakat basittir [6].

IV. ZEKİ STS'LER

Bilgisayar veya ağ sistemlerine yapılan saldırıları tespit ederek güvenliğin sağlanması için geliştirilen STS'ler, her ne kadar yapılan saldırıların büyük bir çoğunluğunu tespit edebilseler de daha önce hiç karşılaşılmamış olan saldırıların büyük çoğunluğunun tespit edilememesi ve bu saldırıların sistemlerde büyük zararlara yol açması, yeni saldırı çeşitlerinin tespit edilebilme başarısının artırılması ihtiyacını getirmiştir. Bu ihtiyacın karşılanması ve hızla değişen saldırı tiplerinin karşısında, bilgi ve bilgisayar güvenliğinin sağlanması amacıyla, STS'lerin geliştirilmesinde yapay zeka yöntemleri kullanılarak STS performanslarının iyileştirilmesi hedeflenmiştir. Yapay zeka tekniklerinin öğrenilebilmesi hızlı hesaplama, genelleme matematiksel olarak modellenmesi zor olan problemlere çözüm sunabilmesi gibi özellikler, bu yaklaşımların STS'lerde kullanılmasının önemli gerekçelerindendir. Zeki yaklaşımların kullanılmaya başlaması ile birlikte anormallik tespiti yaklaşımı biraz daha ön plana çıkmış ve bu sayede anormallik tespitinin yeni saldırıları tespit edebilme yeteneği arttırılmıştır.

Yapay zeka araştırmacılarının baştan beri ulaşmak istediği ideal, insan gibi düşünen ve davranan sistemler geliştirmektir. Ancak buna ulaşmanın güçlüğü anlaşılınca çalışmanın yönü rasyonel düşünen ve davranan sistemlerin tasarlanmasına çevrilmiştir. Geleneksel yöntemlerle çözümü zor veya imkansız olan problemlerin çözümünde kullanılan, yapay zeka

teknikleri, yapay sinir ağları, bulanık mantık, sezgisel (genetik, tabu arama, karınca koloni, ısıl işlem (tavlama) benzetimi, bağışıklık sistemi, arı) algoritmalar olarak sıralanabilir.

Bulanık Mantık

Bulanık mantık metodunu uygulama girişimleri, STS'nin farklı bileşenlerinin geliştirilmesi için 2000'li yıllarda başlamıştır. Bu çalışmalarla ortaya çıkan FIRE (Fuzzy Intrusion Recognition Engine) ile ağ verileri işlendikten sonra atakları tespit etmek için bulanık mantık kullanılmıştır [12]. Ağ paketleri üzerinde çalışılan FIRE'de, TCP, UDP ve ICMP için otonom ajanlar kullanılır [20]. Aynı zamanda kural tabanlı bir sistem olan bu çalışmada, güvenlik yöneticisi ve edinilen tecrübe sayesinde belirlenen bulanık kurallar oluşturulmuştur [21]. 2002 yılında bulanık mantığın, anormallik tespiti yapan bir STS'nin karar verme aşamasında kullanılması önerilmiştir [22]. Bu çalışmada bulanık mantık, uzman tarafından tavsiye edilen, bulanık "if-then" kurallarını temel alarak çözüm sunmaktadır.

Genetik Algoritmalar

Genetik algoritmalar STS'lerde, trafik verilerine basit kurallar uygulamak için kullanılabilir. Bu kurallar, anormal trafik verilerinden normal verileri ayırmak içindir. Veri kümesi, tcpdump ya da snort gibi trafik dinleyiciler (sniffers) kullanılarak toplanır [13]. Genetik algoritmalar öncelikle küçük boyutlu rasgele üretilmiş kurallar kümesi ile başlar, daha sonra bu kural kümesi genişletilir.

Yapay Bağışıklık Sistemi

Literatürde insan bağışıklık sistemine dayalı birçok STS çalışması sunulmuştur. Bu çalışmalardan bazıları doğal bağışıklık sistemi karakteristiklerinden esinlenerek, bilgisayar sistemlerinde anormallik tespiti için biçimsel (formal) çatı (framework) önermişlerdir. Doğal bağışıklık sisteminin, bağışıklığı tanımladığını düşündükleri 4 önemli özelliğini kullanmışlardır. Bunlar; farklılık (diversity), doğal dağıtık yapısı (distributed nature), hata toleransı (error tolerance) ve doğal dinamik yapısıdır (dynamic nature) [23].

Destek Vektör Makinaları

DVM'ler STS'lerde, özellik vektörünün seçilmesinde sıkça kullanılmıştır. Hızlı olmaları nedeniyle STS'ler için oldukça kullanışlı bir yöntemdir. DVM'ler geniş bir örnek setini öğrenebilir ve iyi ölçeklendirirler [24].

Yapay Sinir Ağları

Zeki yaklaşımların STS'lerde kullanılmaya başlaması, farklı birçok zeki yöntemin de kullanılabilir olduğunu göstermiştir. Bu tekniklerden hemen hemen hepsi STS'lerin geliştirilmesi için kullanılmış olsa da, elde edilen başarılı sonuçlardan dolayı en çok kullanılanlardan biri YSA'dır [25, 26].

YSA'lar, giriş ve çıkış vektörleri arasında ilişki kurarak kendi algoritmalarını uygularlar ve genelleştirerek yeni giriş/çıkış ilişkilerini ortaya çıkarırlar. Bu yaklaşım, sistemdeki kullanıcıların davranışlarının öğrenilmesiyle gerçekleşir. Spesifik bir kullanıcı için önceki komutlardan yola çıkarak yeni komutu tahmin eder.

V. YSA'NIN STS'LERDE KULLANILMASI

Yapay sinir ağları (YSA), saldırı tespit sistemlerinde 1990'ların başında kullanılmaya başlanan zeki yaklaşım yöntemlerinden biridir. YSA'lar, anormallik tespiti yapan STS'ler için istatistiksel yöntemlere alternatif olarak önerilmiştir [26].

YSA'ların STS'lerde kullanımı, YSA'nın normal sistem davranış izleriyle eğitilmesi ile başlar. Normal veya anormal olarak sınıflandırılan olay akışları yapay sinir ağına verilir. Toplanan veriler ile sistemin davranışına bağlı olarak öğrenme değişimi yapılabilir. Yani eğitim, izin veriliyorsa sürekli hale getirilebilir. Buradaki yaklaşım, kullanıcının n adet hareket veya komutundan, sonraki hareket veya komutunun tahminen eğitilmesidir [18]. Bu tahminin yapılması için öncelikle eğitim veri seti oluşturulmalıdır, daha sonra da eğitim tamamlanmalıdır. Eğitim verileri, belirli zaman periyodunda (birkaç gün) her kullanıcı için, sistem hesaplarından toplanır. Her gün ve her kullanıcı için veriler vektörel forma sokulur ki bu vektör kullanıcının her komutu ne kadar sıklıkta yürüttüğünü gösterir. Eğitim aşamasında ise daha önce elde edilen vektörler, kullanıcıları tanımlamak için eğitilir.

YSA'lar, anormallik tespitinde kullanıldığı gibi kötüye kullanım tespitinde de kullanılan bir tekniktir. Ağ ataklarının sürekli değişen yapısı, ağ trafiğini geniş çapta analiz edebilen ve kural tabanlı sistemlerden daha esnek bir savunma sistemi ihtiyacını doğurmuştur. YSA tabanlı kötüye kullanım tespiti yapan sistemlerle, kural tabanlı sistemlerde var olan bu tür problemlere çözüm sağlanabilmektedir [26].

YSA'lar, kötüye kullanım tespitinde iki farklı şekilde kullanılmaktadır [26]. İlk yaklaşımda yapay sinir ağları, zaten var olan bir uzman sistemin bir parçası olarak kullanılmaktadır. Bu yaklaşımda, saldırı tespitinin daha etkin yapılması amacıyla gelen verilerin filtrelenmesi ve uzman sisteme gönderilmesinde YSA'lardan faydalanılır. İkinci yaklaşımda ise, YSA'lar tek başına bir sistem olarak kötüye kullanımı tespit etmekte kullanılır. Bu yaklaşımda YSA, ağ akış bilgilerinden, kötüye kullanım tespitinin analizinde kullanılır.

YSA'lar, STS'lerde karşılaşılan pek çok problemlere esnek çözümler sunabilirler, YSA'nın çözüm sunduğu temel iki problem, veri redaksiyonu ve sınıflandırmadır [27]. Veri redaksiyonu (azaltma), işleme zamanını, iletişim yükünü ve depolama gereksinimlerini azaltmak amacıyla veri koleksiyonunu analiz ederek en önemli girişleri tanımlama işidir. Sınıflandırma ise saldırganları ve atak yapanları tanımlama işlemidir. YSA'lar pek çok STS'lerde bu iki önemli problemi çözmek için kullanılmışlardır [27].

STS'lerde karşılaşılan diğer problemler, istatistiksel yayılımı doğrulama ihtiyacı, tespit ölçütlerinin değerlendirilmesinin zorluğu, algoritma geliştirmenin yüksek maliyeti ve ölçeklemede zorluk olarak sıralandırılabilir [28].

YSA'lar bu problemlere de çözüm sağladığından dolayı STS'ler için oldukça uygun bir tekniktir.

YSA'nın STS'lerde kullanılmasının avantajları

(1) Kötüye kullanım ataklarının karakteristiğini öğrenmesi ve daha önce ağda kaydedilen örneklere benzemeyenleri ayırt edebilmesi,
(2) Hızlı sonuç üretmesi sayesinde gerçek zamanlı uygulamalar için kullanışlı olması,
(3) Gürültülü verilerle de çalışabildiklerinden, gürültülü verilerin sonuçları diğer yöntemlere göre daha az bozması,
(4) Farklı sistemlerle beraber çalışabilmeleri,
(5) Genel olarak çözüm sağlayabilmeleri yanında kısmi olarak da STS'lerin tasarımında kullanılabilmeleri,
(6) Az örneklerde sistemin veya atağın genel davranışını öğrenebilme yetenekleri olarak sıralanabilir.

Tüm bu avantajların yanı sıra, en büyük problem yapay sinir ağlarının eğitilmesidir. Yapay sinir ağı, etkin şekilde çalışması için iyi eğitilmelidir ve geniş bir veri seti kullanılmalıdır [1].

VI. Bilgi Güvenliğinde STS'lerin Önemi

İnternetin ve iletişim olanaklarının artmasıyla birlikte saldırganlar tarafından saldırılabilecek daha çok sistem ortaya çıkmıştır. Bu saldırıların büyük bir bölümü kullanılan sistemin kusurları veya eksiklerinden faydalanılarak yapılır. Bu tür saldırıları engellemenin iki yolu vardır; ilki tamamen güvenli bir sistem ve ortam oluşturmak, ikincisi ise saldırıları tespit edip gerekli önlemleri almaktır. Bunlardan ilki pratik açıdan mümkün olmamaktadır. Bunların gerekçeleri ise [18],

- Kullanılan işletim sisteminde var olan açıkların genellikle ilk olarak saldırganlar tarafından fark edilmesi ve önlem alınana kadar bu açıkların kullanılabilmesi,
- Veri iletiminde kullanılan protokollerin yapısında var olan bazı kuralların saldırı amaçlı kullanılabilmesi,
- Kriptografik metotların ve anahtarlarının kırılabilmesi, kullanıcıların şifrelerini unutabilmesi veya kripto-sistemin kırılabilmesi gibi nedenlerle yüksek seviyede bir güvenlik sağlanamaması,
- Dış ortama karşı güvenliği sağlanan sistemin, iç ortamlardan suistimal edilerek güvenliğin ortadan kaldırılması,
- Güvenlik amacıyla kullanıcı yetkilerinin minimuma indirilmesi sonucu kullanıcı verimliliğinin düşmesi gibi nedenleri vardır.

Sistemlerini korumak isteyenler, genelde saldırı gelene kadar bekleme pozisyonunda kalmak, saldırı geldiğinde ise olabildiğince hızlı tespit etmek isterler. Bu ise STS'nin yaptığı iştir [18]. Bir saldırının hangi adresten veya hangi porttan geldiğini bilmeden engel olmak mümkün değildir. STS'ler saldırıları tespit ederken bu bilgileri de elde ederler. STS'ler, detaylı olarak topladığı ve depoladığı bilgilerden yararlanarak, saldırıları olabildiğince erken tespit etme özelliğine sahiptir. Yine aynı bilgilerin incelenmesi ile daha önce hiç karşılaşılmamış bir saldırıyı da tespit edebilir. STS'leri de cazip hale getiren bu özelliktir.

VII. Sonuç ve Değerlendirmeler

Bu çalışmada, STS'ler genel olarak incelenmiş, STS'lerde kullanılan klasik ve zeki teknikler gözden geçirilmiştir.

Literatür incelemesinden elde edilen bilgiler doğrultusunda, çalışma genel olarak değerlendirildiğinde;

- Ülkemizde zeki saldırı tespit sistemlerine yönelik yeterli çalışma bulunmadığı,
- Ülkemizde geliştirilecek olan STS'lerin testinde kullanılabilecek bir veri kümesi bulunmadığı,
- Literatürde, veri kümesi oluşturmak için yapılan çalışmaların güncel olmadığı tespit edilmiştir.

Bu araştırmada elde ettiğimiz bilgi ve deneyimlere dayanarak, saldırıları tespit etme yöntemlerine göre ikiye ayrıldığını bildiğimiz STS'lerin, hangi yöntemin seçileceğine dair dikkat edilmesi gereken noktası, anormallik tespiti yönteminin, bütün kötü davranışları tespit etmeye çalışırken, kötüye kullanım tespiti yönteminin kötü olarak bilinen davranışları tanımaya çalışmak olduğudur. Her iki yöntemin de avantaj ve dezavantajları olduğu göz önünde bulundurularak, tasarımlarda avantajları bir araya toplayan hibrit yaklaşımlardan faydalanmanın daha gerçekçi olacağı değerlendirilmektedir.

KAYNAKLAR

[1] Ş. Sağıroğlu, M, Alkan, "Her yönüyle elektronik imza (e-imza)", Grafiker Yayınları, Ankara, 1-100 (2005).
[2] D. E. Denning, "An intrusion detection model", IEEE Transactions on Software Engineering, 13(2): 118–131 (1987).
[3] B. Mukherjee, L. T. Heberlein, K. N. Levitt, "Network intrusion detection", IEEE Network, 8(3): 26-41 (1994).
[4] M. Crosbie, E. H. Spafford, "Defending a computer system using autonomous agents", Technical Report 95-022, Dept. of Comp. Sciences, Purdue University, West Lafayette, 1-11 (1995).
[5] D. Endler, "Intrusion detection applying machine learning to solaris audit data", 1998 Annual Computer Security Applications Conference (ACSAC'98), 268-269 (1998).
[6] S. Axelsson, "Intrusion detection systems: A survey and taxonomy", Technical Report 99-15, Dept. of Computer Eng., Chalmers University of Technology, Göteborg, Sweden, 1-23 (2000).
[7] A. Patcha, J. M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends", Computer Networks, 51(12): 3448-3470 (2007).
[8] D. Anderson, T. F. Lunt, H. Javitz, A. Tamaru, A. Valdes, "Detecting unusual program behavior using the statistical component of the next-generation intrusion detection expert system (NIDES)", SRI-CSL-95-06, Menlo Park, California, 1-22 (1995).
[9] C. Endorf, E. Schultz, J. Mellander, "Intrusion Detection & Prevention", Jenn Tust, Jody McKenzie, Elizabeth Seymour, McGraw-Hill, California, 10-150 (2004).
[10] T. F. Lunt, "Automated audit trail analysis and intrusion detection: A survey", 11th National Computer Security Conference, Baltimore, MD, 65-73 (1988).
[11] S. A. Hofmeyr, "An immunological model of distributed detection and its application to computer security", Doktora Tezi, Computer Science, University of New Mexico, 1-69 (1999).
[12] J. E. Dickerson, J. A. Dickerson, "Fuzzy network profiling for intrusion detection" NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, Atlanta, 301-306, (2000).

[13] A. Murali, M. Rao, "A survey on intrusion detection approaches", First International Conference on Information and Communication Technologies, IEEE Communications Society Press, 233-240 (2005).
[14] A. K. Jones, "Computer System Intrusion Detection: A Survey", Technical Report, Computer Science Dept., University of Virginia, Charlottesville, Virginia, 1-21 (2000).
[15] W. Lee, S. J. Stolfo, P. K. Chan, E. Eskin, W. Fan, M. Miller, S. Hershkop, J. Zhang, "Real time data mining-based intrusion detection", Second {DARPA} Information Survivability Conference and Exposition (DISCEX II), Anaheim, CA, 89-100 (2001).
[16] K. Ilgun, R. Kemmerer, P. Porras, "State Transition Analysis: A RuleBased Intrusion Detection System", Software Engineering, 21(3): 181-199 (1995).
[17] İnternet: Knowledge Discovery and Delivery, "KDD Cup 1999: General Information",http://www.sigkdd.org/kddcup/index.php?section=1999&method=info (2007).
[18] A. Sundaram, "An introduction to intrusion detection", Crossroads: The ACM Student Magazine, New York, USA, 2(4), 3-7 (1996).
[19] P. A. Porras, "STAT: A State Transition Analysis Tool for intrusion detection", Yüksek Lisans Tezi, Computer Science Department, University of California, Santa Barbara, 1-150 (1992).
[20] J. E. Dickerson, J. Juslin, O. Koukousoula, J. A. Dickerson, "Fuzzy intrusion detection", IFSA World Congress and 20th North American Fuzzy Information Processing Society (NAFIPS) International Conference, Vancouver, British Columbia, 3: 1506-1510 (2001).
[21] K. Lee, L. Mikhailov, "Intelligent Intrusion Detection System", Second IEEE International. Conference on Intelligent Systems, 2: 497-502 (2004).
[22] S. B. Cho, "Incorporating soft computing techniques into a probabilistic intrusion detection System", IEEE Transactions on Systems, Man, and Cybernetics, Part C 32(2): 154-160 (2002).
[23] F. Esponda, S. Forrest, P. Helman, "A formal framework for positive and negative detection schemes", IEEE Transactions on Systems, Man, and Cybernetics, Part B, Cybernetics, 34(1): 357-373 (2004).
[24] S. Mukkamala, A. H. Sung, A. Abraham, "Intrusion detection using ensemble of soft computing paradigms", Third International Conference On Intelligent Systems Design and Applications, Germany: Springer, 239-248 (2003).
[25] R. E. Wassmer, J. H. Fikus, "Advanced Intrusion Detection Techniques", Final rept., Defense Technical Information Center - ADA410454, 2. evre, 1-14, (2003).
[26] J. Cannady, "Artificial neural networks for misuse detection", Proceedings of the 1998 National Information Systems Security Conference (NISSC'98), Arlington, VA, 443-456 (1998).
[27] J. Frank, "Artificial intelligence and intrusion detection: current and future directions", Division of Computer Science, University of California at Davis, 1-12 (1994).
[28] S. Peddabachigari, A. Abraham, C. Grosan, J. Thomas, "Modeling intrusion detection system using hybrid intelligent systems", Journal of Network and Computer Applications, Elsevier, 30:114–132 (2007).