TCP SYN Seli Saldırılarının Bulanık Mantık Kullanarak Tespiti

Taner Tuncer, Yetkin Tatar

***Özet*— Ağ güvenliğinde en büyük problemlerden biri Servis Yalanlama (Denial of Service, DoS) saldırılarıdır. DoS saldırıları günümüzde en yaygın kullanılan saldırı biçimlerinden biridir. Çünkü bir çok saldırı yöntemini içinde barındırır. Genelde bir ağa yada kaynağa ulaşımı engellemek için kullanılan DoS saldırılarının en yaygın olarak bilineni TCP SYN seli saldırılarıdır. Bu saldırılarda normal TCP SYN paketi, saldırı paketinden ayırt edilemez. Bu makalede TCP SYN seli saldırılarının tespiti için Bulanık Mantık Tabanlı bir sistem önerilmiştir. Değerlendirme sonuçlarında, önerilen sistem Adaptif Eşik Değer algoritması ile karşılaştırılarak düşük ve yüksek yoğunluktaki saldırıları doğru tespit ettiği gösterilmiştir.**

***Anahtar Kelimeler*— TCP SYN Seli, Adaptif Eşik Değer Algoritması, Bulanık Mantık.**

I. GİRİŞ

İNTERNET kullanımı son yıllarda hızla artıyor. İnternetteki hızlı büyüme ve kullanım internet güvenliğinin sağlanmasını da beraberinde getirmektedir. Güvenliğin az veya zayıf olması durumunda servis sağlayıcılarında ve kurumlarda ciddi hasarlar olabilmektedir. Geçmişte Yahoo ve eBay gibi ticari siteler DoS gibi saldırılarına maruz kalarak, servisleri kullanılamaz hale gelmiş ve büyük miktarlarda maddi zarara uğramışlardır[1].

İnternette gerçekleştirilen en yaygın saldırılar DoS saldırılarıdır. DoS saldırıları karşı sistemde çalışan servisin durdurulmasını amaç edinir ve yasal kullanıcıların hizmet almasını engeller. Bu saldırılar iki şekilde servisi durdurabilir. İlki işlemçi, hafıza, bant genişliğini sonuna kadar kullanmak diğeri ise sistemdeki bir zayıflığı kullanarak servisi durdurmaktır. UDP seli, ICMP seli, TCP SYN seli gibi saldırılar DoS saldırılarından başlıcalarıdır[1]. TCP SYN seli saldırıları TCP/IP protokol açıklarından faydalanılarak gerçekleştirilir. Internete bağlı TCP protokolü tabanlı iletişim gerçekleştiren web, e-post, ftp gibi sunucular bu tür saldırılara maruz kalmaktadır[1,2]

UDP ve ICMP seli saldırılarında saldırgan birçok paket oluşturarak kurbana gönderir[1]. Kurbanın ağ bağlantı kapasitesi tüketilir. TCP SYN seli saldırısında ise saldırgan sunucuya birçok bağlantı isteğinde bulunur[1]. Eğer bağlantı isteği sunucunun hizmet verebileceği oturum sayısından fazla olur ise sunucu, gelen yeni istekleri reddeder ve DoS saldırısı başarılı olmuş olur. Bütün DoS saldırılarının %90 ı TCP SYN seli saldırısı iken DoS saldırılarının %55 i ise web sunucularına gerçekleştirilen saldırılardır[3].

Genel olarak DoS saldırılarının tespitinde İstatistiksel yöntemler uygulanır[2,3,4]. Literatürde DoS saldırılarını tespit etmek için Adaptif Eşik Değer algoritması, Kümülatif Toplam algoritması, Eşik Değer Ölçüsü ve İstatistiksel Momentler kullanılır[2,3,4,5,7]. İlk üç yöntemde uygun eşik değer belirlenmesi için gerekli parametrelerin belirlenmesi başlıca problem iken istatistiksel momentler kullanılarak saldırı tespitinde ise ağ trafiğinin modellenmesi başlıca problemi teşkil eder. Tüm bu yöntemlerde amaç DoS saldırılarının erken ve doğru tespit edilmesidir.

Bu makalede TCP SYN saldırılarının tespiti için Bulanık Mantık Tabanlı bir sistem önerilmiştir. Bu amaç için makalenin geri kalan kısımları aşağıdaki gibi organize edilmiştir. Bölüm II' de TCP oturumunun nasıl gerçekleştirildiği anlatılarak TCP SYN seli saldırılarının yapısından bahsedilmiştir. Bölüm III' te Adaptif Eşik Değer algoritması anlatılarak, Bulanık Mantık ile TCP SYN seli saldırılarının nasıl tespit edileceğine dair önerilen sistem ve saldırı tespitindeki klasik yöntemlerden olan Adaptif Eşik Değer algoritması açıklanmıştır. IV. Bölümde gözlemlenen ağ trafiği özellikleri açıklanmış, hem Adaptif Eşik Değer algoritması hemde önerilen sistem için deneyler gerçekleştirilmiştir. Sonuç bölümünde ise sistemin avantaj ve dezavantajlarından bahsedilmiştir

II. TCP SYN SALDIRILARI

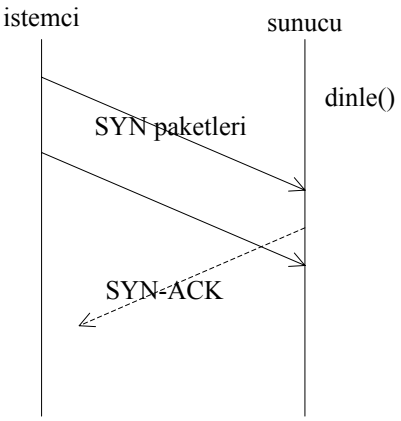
TCP protokolü iki bilgisayar arasında veri transferi yapılmadan önce bağlantı kurulumu ve veri iletiminin garantili olarak yapıldığı bir protokoldür[6]. Bir istemci bir sunucu ile TCP bağlantısı kurmak istediğinde el sıkışma olarak adlandırılan 3 aşamalı süreç gerçekleştirilir[1,6]. Birinci aşamada istemci sunucuya TCP SYN paketi gönderir. Bağlantı isteğini alan sunucu istemciye TCP SYN/ACK onay paketini gönderir. TCP SYN/ACK paketini alan istemci bağlantı kurulumunun son aşamasında sunucuya TCP ACK paketi göndererek iletişimi başlatıp veri transferine başlar. Aynı şekilde bağlantının sonlandırılması ise TCP FIN, ACK, FIN, ACK paketlerinin istemci ve sunucu arasında karşılıklı olarak gönderilmesiyle bağlantı normal yollarla sonlandırılır.

T. T., Fırat Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde görev yapmaktadır. tel: 424 3270000/5231 fax: 424 2181907 e-mail: ttuncer@ firat.edu.tr

Y. T., Fırat Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde görev yapmaktadır. tel: 424 3270000/5228 fax: 424 2181907 e-mail: ytatar@ firat.edu.tr

TCP genelde güvenli bir iletişim ortamı sağlamasına rağmen bağlantı kurulumu aşaması dezavantajlar içerir. Bu dezavantajlardan biri TCP SYN seli saldırılarına olanak vermesidir. Bu saldırılarda, normal TCP SYN paketi, saldırı paketinden ayırt edilemez. Bağlantı kurulumu aşamasında sunucu istemciye TCP SYN/ACK paketini göndererek bağlantı için hafızada bir yer tahsis eder. Bağlantının bu durumu yarı-açık (half-open) bağlantı olarak adlandırılır. Sunucuda, eğer bir çok yarı-açık bağlantı konumunda bekleyen istek var ise hafıza tükenir. Yeni gelen bağlantı istekleri sunucu tarafından reddedilir.

Şekil.1' de TCP SYN saldırılarının yapısı gösterilmiştir. Saldırgan (istemci) TCP SYN paketlerinin kaynak IP adres alanını spoof ederek sunucuya paketi gönderir. Sunucu TCP SYN paketini alır. Spoof edilen IP numarasına TCP SYN/ACK paketini gönderir. Ağ üzerinde böyle bir IP numarasına sahip istemci olmadığından sunucu bağlantı isteğini TCP ACK paketi gelene kadar bekletir. Bu senaryo gibi birçok bağlantı isteği TCP SYN seli saldırısı olarak adlandırılır.



Şekil.1 TCP SYN saldırısı

Sunucu TCP SYN/ACK paketini 5 kez istemciye göndererek bağlantı kurulumunu gerçekleştirmek ister. Bu tekrar süreleri, 3, 6, 12, 24 ve 48 saniyedir[1]. Sunucu, tahsis etmiş olduğu hafıza alanını boşa çıkartmadan önce, 96 saniye sonra, son bir kez TCP SYN/ACK paketini istemciye gönderecektir. Bu süre zarfında TCP ACK paketi gelmez ise bağlantı isteği hafızadan TCP RST paketi kullanılarak silinir. TCP RST paketleri 2 sebeple üretilir. Birincisi pasif TCP RST kapalı bir porta gelen isteğe karşılık portun kapalı olduğunu belirtmek için kullanılır. İkincisi ise yarı açık durumundaki bağlantının sonlandırılması için kullanılır.

Normal bir ağ trafiğinde TCP SYN paketleri TCP SYN/ACK paket sayıları birbirine eşittir. Gerçek ağ ortamı böyle değildir. Saldırı esnasında TCP SYN/ACK paket sayısı TCP SYN paketlerinden daha fazladır. Literatürdeki algoritmalar ile, TCP SYN, SYN/ACK, oturum sonlandırma paketleri (FIN), RST kullanılarak saldırı tespiti gerçekleştirilmiştir[2,3,4,5,7].

III. Adaptif Eşik Değer Algoritması ve Önerilen Sistem

A. Adaptif Eşik Değer Algoritması

Trafik akışındaki saldırıları tespit etmek için geliştirilen bu algoritmada belirlenen bir eşik değerin aşılıp aşılmamasına göre alarm üretilir. x_n, n. zaman aralığında TCP SYN paketlerinin sayısı , n. zamandan bir önceki ortalama değer ise, Algoritma aşağıdaki şart ile alarm üretir.

Eğer $x_n \geq (\alpha+1)\mu_{n-1}$ O zaman (1)

Burada α parametresi ortalama değerin üstündeki yüzdeyi yani anormallik davranışı belirler. , geçmiş zaman dilimlerindeki ölçümlerle EWMA (Exponential Weighted Moving Average) kullanılarak hesap edilir.

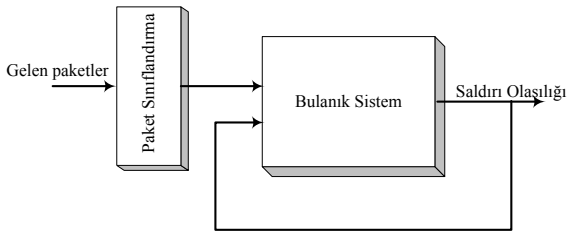
$$\mu_n = \beta\mu_n + (1-\beta)x_n \quad (2)$$

Burada β, EWMA faktörüdür. Bu algoritmanın yanlış alarm sayısı yüksektir. Algoritmanın zorluğu α, β ve k parametrelerinin doğru bir şekilde belirlenebilmesidir. k, ardışık zaman aralıklarının sayısını göstermek üzere, genel olarak alarm şartı aşağıdaki gibi verilir.

Eğer $\sum_{i=n-k+1}^{n} 1_{\{x_i \geq (\alpha+1)\mu_{n-1}\}} \geq k$ O zaman Alarm (3)

B. Önerilen Sistem

Bulanık mantık belirsizlik ve kesinsizlik içeren sistemlerin çözümünde kolaylık sağlayan bir esnek hesaplama yöntemidir. Bu nedenle bulanık mantık lineer olmayan sistemlere yaklaşım yapabilmek için uygundur. Ağ trafiği nonlineer bir özellik taşır. Çünkü ağ trafiği patlamalı bir özellik gösterir. Ağ trafiğini modellemek ve ağ trafiğinin davranışını zaman üzerinde tahmin etmek zor bir problemdir. Ağa yapılan saldırılarında ne zaman yapılacağı belirsizlik içerir. Bu saldırıların gerçek ağ trafiği içerisinde belirlenebilmesi de ayrı bir problemdir. Bu makalede TCP SYN seli saldırılarını sezmek için bulanık mantık tabanlı şekil.2' deki sistem önerilmiştir.

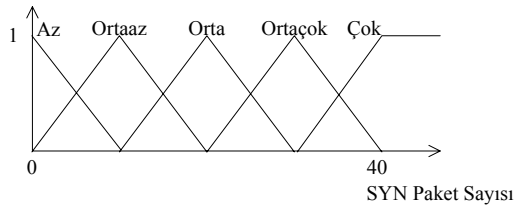


Şekil.2 Önerilen Sistem

Önerilen sistem 2 blok içermektedir. İlk blok gelen ağ trafiği paketlerinin sınıflandırma işlevini yerine getiren Paket Sınıflandırma bloğudur. Bu blok bir sunucuya gelen paketlerin toplanması ve sınıflandırılması görevini yapmaktadır.

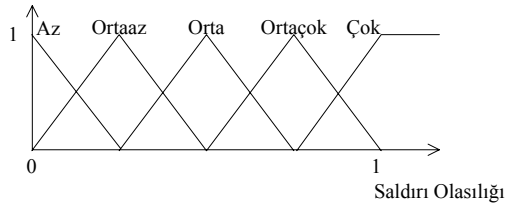
Yakalanan her bir paketin başlık bölümleri kontrol edilerek TCP paketi (SYN) olup olmadığına karar verilir. Başlık bölümünde fragment ofset değeri eğer sıfır ise paket TCP paketidir. Bu TCP paketi için bayrak bitlerinden SYN bayrağı eğer bir ise paket TCP SYN paketidir. Paket sınıflandırma bloğu belirlenen bir Δt zaman aralığında TCP SYN paketlerini toplayarak bulanık sistem girişine verir. Bu ise önerilen sistemin ikinci bloğudur. Bu makalede Δt zamanı 5 saniye olarak alınmıştır.

Bulanık Sistem ise geri besleme girişi ve TCP SYN paket trafiğinden oluşan toplam 2 girişe sahiptir. Bu blok TCP SYN seli saldırısının tespitinden sorumludur. Paket sınıflandırma sisteminden gelen ağ trafiği TCP SYN paketlerinin sayısıdır. Bu girişe ait üyelik fonksiyonları {Az, Ortaaz, Orta, Ortaçok, Çok } şekil.3' deki gibidir.



Şekil.3 TCP SYN paket sayısı üyelik fonksiyonu

Sistemin diğer girişi ise aynı zamanda saldırı tespit olasılığı değerini göstermektedir. Sistemin başlangıç anındaki değeri ise sıfırdır. Saldırı olasılığı, şekil.4' te gösterildiği gibi 0-1 aralığında 5 üyelik fonksiyonuna { Az ,Ortaaz, Orta, Ortaçok, Çok} sahiptir. Sistemin geri beslemeli olmasındaki amaç Δt zamanı önce ağın hangi durumda olduğunun yani saldırının olup olmadığının bir sonraki zaman dilimine aktarılmasıdır. Bu geri besleme bize saldırının başlangıç zamanını tespit edebilmeye yardım edecektir.



Şekil.4 Saldırı olasılığı üyelik fonksiyonu

Sistem saldırı tespitinde kullanılmak üzere toplam 25 kural içermektedir. Aşağıda sistemin kullandığı birkaç kural verilmiştir.

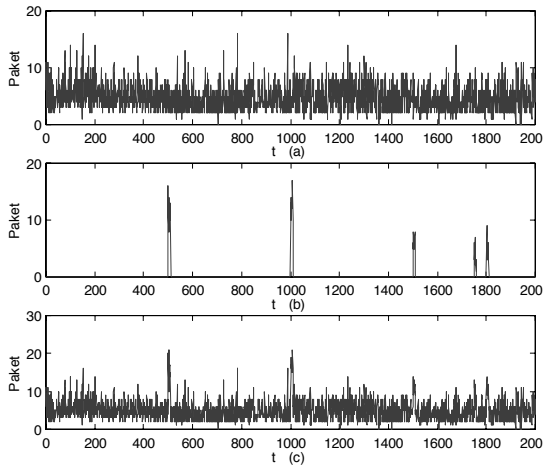
Eğer SYN paket sayısı=Az ve Saldırı olasılığı=Çok ise o zaman Saldırı olasılığı orta' dır.

Eğer SYN paket sayısı=Çok ve Saldırı olasılığı=Çok ise o zaman Saldırı olasılığı Çok' tur.

Eğer SYN paket sayısı=Orta ve Saldırı olasılığı=Az ise o zaman Saldırı olasılığı Ortaaz' dır.

IV. UYGULAMA

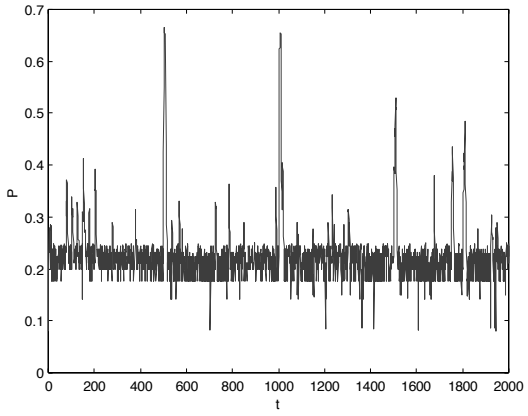
TCP SYN seli saldırısı tespiti için Fırat üniversitesi web sunucusuna gelen bağlantı isteği için trafik ölçümleri kullanılmıştır. Bu amaç için Etheral paket programı kullanılarak port 80' e gelen TCP paketi (SYN bayrağı 1) her 5 saniyede bir toplanmıştır. Yaklaşık olarak 3 saatlik bir zaman dilimindeki bağlantı isteklerinin değişimi elde edilmiştir. Δt zaman aralıkları için ortalama paket yoğunluğu 6,4 pakettir. Elde edilen bu bağlantı istekleri normal isteklerdir. TCP SYN seli saldırısı için yapay olarak üretilmiş TCP SYN bayraklı paketler oluşturulmuş ve Web sunucusuna bir tek noktadan saldırı yapılmıştır. Aşağıdaki şekil.5 (a) normal TCP SYN paket trafiğini, şekil.5 (b) Sunucuya yapılan saldırı trafiği değişimini, şekil.5 (c) zaman üzerinden saldırı trafiğini de içeren TCP SYN paketlerinin değişimini göstermektedir.



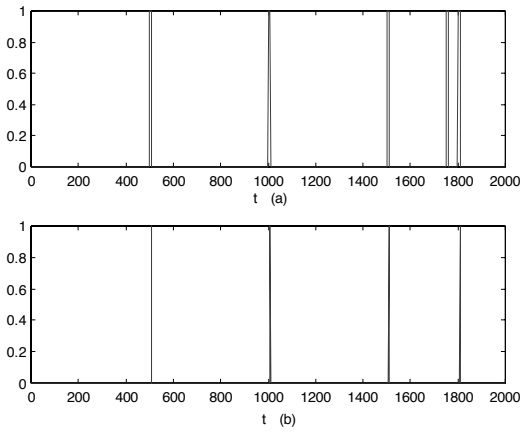
Şekil.5 Gözlemlenen ağ trafiği

Saldırılar 500, 1000, 1500, 1750 ve 1800. Δt zamanlarında gerçekleştirilmiştir. Bu saldırılardan ilk ikisi yüksek yoğunluktaki saldırılardır. Son üç saldırı ise düşük yoğunluktaki saldırıyı temsil etmektedir. Yüksek yoğunluktaki saldırılar, normal ağ trafiğinin ortalama değerinin yaklaşık 2 katı büyüklüğündedir. Düşük yoğunluklu saldırılar ise normal trafiğinin ortalama değerinin 1.1, 0.9 ve 1.0 katı yoğunluktadır. Önerilen sistemin, gözlem aşamasında elde edilen saldırı olasılığı değişimi şekil.6 da verilmiştir.

Şekil.7'de, önerilen Bulanık Mantık Tabanlı sistemden ve Adaptif Eşik Değeri algoritmasından elde edilmiş saldırı alarmları gösterilmiştir. Her iki yöntem içinde aynı paket trafik yoğunluğu kullanılmıştır. Önerdiğimiz sistem ile hem yüksek hem de düşük yoğunluktaki saldırı olasılığı belirgin bir şekilde elde edilerek tüm saldırılar tespit edilmiştir. Adaptif Eşik Değer algoritmasında ise kullanılan parametreler α, β ve k sırasıyla 0.5, 0.995 ve 10 olarak alındığında, şekil.7 (b)' de görüldüğü gibi yapılan saldırılardan yalnızca 4 tanesi belirlenmiştir.



Şekil.6 Saldırı olasılığı değişimi



Şekil.7 Tespit edilen saldırılar

Önerdiğimiz sistemde olasılık için eşik değerin belirlenmesi ayrı bir problemdir. Ancak normal ağ trafiğindeki değişimlerde trafik yoğunluğu bazı zaman dilimlerinde ortalama trafiğin yaklaşık 1,5-2 katı aralığındadır. Bu zaman dilimlerinde belirlenen saldırı olasılık değerleri şekil 4.2 de görüleceği üzere yaklaşık olarak 0,42 ten büyük değildir. Saldırıların yapıldığı zaman aralıklarında ise saldırı olasılığı 0,47 değerinden büyüktür. Ayrıca sistemin geri beslemeli olmasından dolayı saldırı zamanları da saldırı başlangıcından itibaren yüksek doğruluk ile tespit edilmiştir.

V. SONUÇLAR

Ağ tasarımında göz önünde tutulması gereken en önemli konu güvenliktir. Güvenliğin göz önünde tutulmaması durumunda maddi ve manevi zararların olması kaçınılmazdır. Güvenliğin yüksek seviyede tutulması yüksek maliyet ve hız için problem teşkil edebilmektedir. Aksi durumda da servislerin devre dışı kalabilmesi olasıdır. Ağ güvenlik tedbirleri her ne şartta olursa olsun saldırıları erken ve hatasız tespit edebilmelidir. Önerilen sistemde kuralların ve üyelik fonksiyonlarının doğru seçimi, sistemin doğru çalışmasını etkileyen en önemli faktörlerdir. Yine saldırının kesin olarak var olduğunu belirleyen eşik değerinin tespiti de oldukça önemlidir. Genel olarak tüm algoritmalarda, eşik değerin düşük seçilmesi normal ağ trafiğindeki patlamaları saldırı olarak belirlerken yüksek seçilmesi durumunda ise gerçek saldırıların tespit edilememesi durumunu ortaya çıkarır.

KAYNAKLAR

[1] B.Harris, R. Hunt, "TCP IP Security Threats and Attack Methods", Elseiver, Computer Communications (22), sayfa: 885-897, 1999.
[2] V. A. Siris, Fotini P. "Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attack", Elseiver, Computer Communications(29), sayfa:1433-1442, 2006.
[3] H. Wang, D. Zang, K.G. Shin, "Detecting SYN Floofing Attacks" Proceedings of IEEE INFOCOM02, 2002.
[4] R.B.Blazek, H. Kim, B.Rozovskii, A. Tartakovsky, " A Novel Approach to Detection of Denial of Service Attacks via Adaptive Sequential and Batch Sequential Change Point Detection Methods, Proceedings of IEEE Workshop on Systems Man and Cybernetics Information Assurance, 2001.
[5] Y. Oshita, S. Ata, M. Murata, " Detecting Distrubuted Denial of Service Attacks by Analyzing TCP SYN Packets Statistically", sayfa:2043-2049 Globecom2004.
[6] http://www.faqs.org/rfcs/rfc793.html.
[7] H. Wang, D. Zang, K.G. Shin, " Change-Point Monitoring for the Detection of DoS Attacks", IEEE Transaction on Dependable and Secure Computing, vol:1 No:4, sayfa:193-208, 2004.

Taner Tuncer, Fırat Üniversitesi Elektrik Elektronik Mühendisliği bölümünden 1996 yılında mezun oldu. 2003 yılında Fırat Üniversitesi Fen Bilimleri Enstitüsünde Yüksek Lisansını tamamlayarak aynı yıl doktora çalışmalarına başladı. İlgi alanları ağ performans tahmini ve ağ güvenliğidir.

Yetkin TATAR, EDMMA Elektrik Mühendisliği bölümünden 1976 yılında mezun oldu. 1983 yılında Yüksek Mühendis, 1994 yılında Doktor unvanını Fırat Üniversitesi Fen Bilimleri Enstitüsünden aldı. İlgi alanları Güç Elektroniği, Sayısal Sistemler, Sayısal İşaret İşleme ve Bilgisayar Ağlarıdır.