DDoS Tespiti ve Trafik Öznitelikleri Seçimi

Derya Erhan[1], Emin Anarım[1], Güneş Karabulut Kurt[2]

[1] Boğaziçi Üniversitesi Elektrik Elektronik Bölümü, İstanbul

[2] İstanbul Teknik Üniversitesi Elektrik Elektronik Bölümü, İstanbul

derya.erhan@boun.edu.tr,
anarim@boun.edu.tr
gkurt@itu.edu.tr

Özet: Dağıtık hizmet engelleme saldırıları günümüzde bilişim sistemleri için ciddi bir tehdit oluşturmaktadır. Bu çalışma dağıtık hizmet engelleme saldırılarından birisi olan veri iletim kontrolü protokolü senkronizasyon paketi baskını saldırılarının, ağ trafiğine ait çeşitli öznitelikler üzerindeki etkisini incelemektedir. DETER test ortamı kullanılarak yapılan benzetimlerden elde edilen çeşitli öznitelikler kümesinden bilgi kazancı kullanılarak, dört ana öznitelik seçilmiştir. Farklı öznitelikler özbağımlı (AR) süreç ile modellenerek elde edilen artıklar oranlanarak bir olağandışılık dizisi elde edilir. Her öznitelikten elde edilen olağandışılık dizileri ve ilinti katsayısı matrisi kullanılarak tek boyutlu bir dizi olan ağ sağlık fonksiyonu hesaplanmıştır. Bu fonksiyon eşiklenerek saldırının başlangıç ve bitiş noktaları tespit edilmiştir.

Anahtar Sözcükler: DDoS, Ağ Güvenliği, Zaman Serisi Modellemesi, AR Model, Bilgi Kazancı.

DDoS Detection and Selection of Traffic Features

Abstract: Distributed denial of service attacks pose an immense threat to the information systems. In this work the effect of transmission control protocol synchronization packet flood attacks on traffic features are examined. Four main features are selected using information gain calculation from a feature set obtained from DETER testbed experiments. Four selected features are modeled using autoregressive modeling and residuals are compared in order to obtain abnormality vector. All abnormality vectores obtained from features are combined with correlation coefficient matrix to obtain a one dimensional traffic health function. By applying threshold to traffic health function start and end times are detected.

Keywords: DDoS, Network Security, Time Series Modelling, AR Model, Information Gain.

1. Giriş

Dağıtık kaynak engelleme (DDoS) saldırıları hedef alınan sistem servislerinin erişilebilirliğini engelleyen eş güdümlü bir saldırıdır.

Bu çalışma, bir DDoS saldırı çeşidi olan veri iletim kontrol protokolü senkronizasyon paketi baskını (TCP SYN flood) saldırısının, belirli trafik öznitelikleri üzerindeki etkisini incelemektedir. Bu etki kullanılarak, ileri düzey bir araştırma yapıldığında, saldırının varlığının yanı sıra saldırı çeşidi de belirlenebilir. Farklı trafik öznitelikleri farklı saldırılar için alarmlar üretmek için kullanılırlar. Bu sebepten mevcut öznitelik kümesinden en verimli öznitelik kümesinin seçilmesi gereklidir.

Bu bildiride, ilk önce DDoS saldırıları ile ilgili genel bilgi verilmektedir. Üçüncü

bölümde bu çalışmada kullanılan trafik özniteliklerinden bahsedilmektedir. Dördüncü bölümde trafik özniteliklerinin bilgi kazancı (ing:information gain) kullanılarak seçilmesi gösterilmektedir. Beşinci bölümde ani değişim tespiti ve trafik sağlık fonksiyonunun hesaplanması anlatılmaktadır. Son olarak, DETER test ortamı ile yapılan benzetimlerden elde edilen sonuçlar açıklanmaktadır.

Sonuç olarak, yapılan benzetimlerde oluşturulan saldırıların oluşturduğu ağ trafikleri kullanılarak hesaplanmış sağlık fonksiyonundan elde edilen alarmlar ile saldırıların başlangıç ve bitiş noktalarının tespit edilebildiği görülmektedir.

2.DDoS Saldırıları

Genellikle DDoS saldırıları iki sınıfa ayrılır: (1) bant genişliği tüketme saldırıları ve (2) kaynak tüketme saldırıları.

Bant genişliği tüketme saldırıları hedef ağı istenmeyen paketlerle doldurarak, normal (saldırı içermeyen) trafiği engeller. Kaynak tüketme saldırıları ise hedef sistemin bilgisayar kaynaklarını tüketmeyi hedefler. Bu çalışmada hedef alınan veri iletim kontrolü protokolü senkronizasyon (TCP SYN) paketi baskını saldırıları, bir kaynak tüketme saldırısıdır.

2.1.Kaynak tüketme saldırıları

Kaynak tüketme saldırıları, bant genişliği tüketme saldırılarından farklı olarak, ağ protokollerini kötüye kullanan paketleri veya bozuk paketleri içerir [1].

Bu paketler hedef sistemde protokollere uygun olarak gelen paketlerden daha fazla kaynak tüketirler. Hedef sistem bu paketleri işlemeye çalışırken, sistemin işlemci ve hafıza gibi kaynakları, normal kullanıcılara hizmet veremeyecek seviyede kilitlenir.

TCP SYN baskın saldırısı bir kaynak tüketme saldırısı çeşididir. Bu saldırıda saldırgan zombi bilgisayarların sahte TCP SYN istekleri göndermelerini sağlar. Bu paketler hedef sistemin bilgisayar kaynaklarını doldurarak, hedef sistemin normal isteklere cevap vermesini engeller.

Bu saldırı, hedef sistem ve saldırgan zombiler arasında üç yönlü el sıkışma protokolünü istismar eder. Saldırgan bilgisayarlar, hedef sisteme, kaynak IP adresleri sahte olan çok sayıda TCP SYN paketi gönderirler. Hedef sistem, bu paketlerde bulunan sahte IP adreslerine ACK+SYN paketleri gönderip, protokolün zaman aşımı süresince gönderdiği paketlere cevap beklemeye başlar. Hedef sistemde her bir SYN ACK paketi için belirli miktarda işlemci ve hafıza kullanılır. Sahte IP adresleri cevap veremediklerinden, hedef sistem hafıza ve işlemci kaynaklarını tüketir. Bu sebepten dolayı hedef sistem normal kullanıcılara hizmet verememeye başlar.

Birçok farklı DDoS saldırı çeşidi olsa da, [2] bu çalışmanın asıl odaklandığı saldırı çeşidi TCP SYN baskını saldırılarıdır.

2.2.DDoS Saldırılarının Tespiti ile İlgili Güçlükler

DDoS saldırılarının tespiti konusunda karşılaşılan en önemli zorluk, saldırı sırasında gelen paketlerin oluşturduğu trafiğin, saldırı içermeyen paketlerden oluşan trafik ile benzerlik göstermesidir.

Ağ yöneticilerinin en önemli ağ izleme yöntemleri, saniyedeki paket sayısı, dakikada gelen ve giden toplam veri boyutu gibi trafik özelliklerini içerir. Ancak bu veriler tek başlarına, TCP SYN baskını saldırısı gibi çok miktarda küçük boyutta paket gönderen saldırıların varlığının tespitinde kullanışlı değildir.

Ağ trafiğine ait birden fazla öznitelikteki değişimin bir arada incelenmesi, saldırının varlığı hakkında tek bir özniteliğin incelenmesine oranla daha kesin bir bilgi sağlayabilir. Örneğin; bir TCP SYN baskını saldırısında, saniyede gelen paketlerin ortalama boyutları, saniyede iletilen toplam paket sayısı ve saniyede üretilen toplam veri

miktarı gibi diğer trafik özellikleri ile ters ilintilidir. Bunun sebebi, ortalama paket boyutu azalırken, toplam paket sayısı ve üretilen toplam veri miktarının artmasıdır.

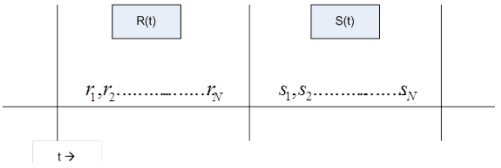
Doğru özniteliklerin seçimi ile saldırı olmayıp kullanıcılardan gelen ağ trafiğinin oluşturduğu ani değişimler ile DDoS saldırılarından oluşan ani değişimler ayırt edilebilir.

3.Ani Değişim Tespiti

İstatistiksel analizde, ağ anomalileri, trafik verisindeki ilintili ani değişiklikler olarak modellenir. Bu bildiride, gözlemin yapıldığı örnekleme aralığında, bir zaman dizisindeki parametrelerin herhangi birindeki değişim, ani değişim olarak tanımlanmıştır. Zaman dizisindeki ani değişiklik, özbağımlı (AR) süreç ile modellenebilir [3]

Thottan, en küçük kare yöntemine dayalı ve ani değişimleri tespit için bir model geliştirmişlerdir. Bu çalışmada, birinci derece özbağımlı süreç en küçük kare modelleme kullanılmaktadır.

Birbirinden farklı özniteliklerin istatistiksel dağılımları da birbirlerinden farklılık gösterdikleri için bu değişkenlerin birlikte işlenmesi zordur. Bu sebepten, ağın iyi halinin tespiti için, farklı trafik özniteliklerinden elde edilmiş anormallik indikatörlerinin birleştirilmesi ile ağ sağlık fonksiyonu [4] hesaplanır. Öznitelik verisi içindeki anormallik, bu verinin istatistiklerindeki ani değişimlerle tespit edilmektedir.



Şekil.1. Parça parça durağan bölümler. R(t) Sağlık fonksiyonu hesaplamak için öncelikle, veri 10 saniyelik parça parça durağan pencerelere ayrılır. *N* uzunluğunda bir zaman penceresi içerisinde *(N=10)*, veri birinci derece AR süreç kullanılarak doğrusal olarak modellenir. Parça parça durağan pencereler R(t) ve S(t) şekil 1 de gösterilmiştir. Daha az ilintili artık elde etmek için birbirleri ile örtüşmeyen pencereler kullanılmıştır $N_R=N_S=10$.

Ani değişimlerin tespiti birbirine komşu iki zaman penceresine AR(1) modellemesi uygulandıktan sonra elde edilen artıkların varyanslarının karşılaştırılması ile yapılır. Her öznitelikteki birer öğrenme ve test penceresinden elde edilen artıklar kullanılarak bir olabilirlik oranı η, aşağıda gösterildiği gibi elde edilir:

$$\eta = \frac{\sigma_R^{-\tilde{N}_R}}{\sigma_R^{-\tilde{N}_R}\sigma_S^{-\tilde{N}_{RS}} + \sigma_R^{-(\tilde{N}_R+\tilde{N}_R)}}. \qquad (1)$$

Burada $\tilde{N}_R = N_R - p$ ve $\tilde{N}_S = N_S - p$, p AR modelin derecesidir. Öncelikle olabilirlik oranlarının bileşenlerinden oluşan bir *(1xn)* uzunluğunda φ dizisi elde edilir. Bu φ dizisi, anormallik dizisidir ve şu şekilde tanımlanır;

$$\varphi = [n_1, \ldots n_n]. \qquad (2)$$

Özgün anormallik dizileri bir sağlık fonksiyonu oluşturmak için bir araya getirilmelidir.

$$\varphi \mathbf{A} \varphi = E(x). \qquad (3)$$

A matrisi, seçilen öznitelikler arasındaki bağıntıya dayanan ve çok boyutlu veriden tek boyutlu bir dizi elde etmemizi sağlayan bir doğrusal bir operatördür. Burada elde edilen E(x), ağ sağlık fonksiyonudur. Sağlık fonksiyonunun aldığı değerlere eşikleme uygulanarak uyarılar üretilmektedir. Bu uyarılar, TCP SYN saldırısının başlangıç ve bitiş anlarının tespiti için kullanılmaktadır.

Thottan [4], sağlık fonksiyonunu hesaplarken kullanılabilecek farklı operatör matrisleri önermiştir. Bunlardan birisi, öznitelikler arasındaki bağıntı katsayı matrisidir. Bu çalışmada **A** operatör matrisi olarak öznitelikler arasındaki bağıntı katsayı matrisi kullanılmıştır. Yapılan çalışmalarda, sağlık fonksiyonu hesaplamasında [4] 'de önerilen diğer operatör matrisleri kullanılsa dahi, ani değişim tespitinde kayda değer farklılıklar görülmemiştir [4].

Operatör matrisi **A** şu şekilde gösterilir;

$$\mathbf{A}=\begin{bmatrix} a_{11} & \dots & a_{14} \\ \dots & \ddots & \dots \\ a_{41} & \dots & a_{44} \end{bmatrix}$$

Saldırı tespiti, ağ sağlık fonksiyonuna eşik değeri uygulanarak üretilen uyarılar sayesinde yapılmaktadır.

4.Trafik Öznitelikleri

Trafik öznitelikleri, ağ üzerinden akan trafiğin içindeki paketlerden elde edilir. Paketler başlık ve yayarlı yük bilgilerini içerirler. Paketlerin içerdiği bu bilgilerden belirli zaman pencereleri, örneğin 1 saniye, kullanılarak farklı öznitelikler elde edilebilir.
Bu çalışmada DETER test ortamında yapılan benzetimlerden elde edilen paketlerin özelliklerinden aşağıdaki öznitelik kümesi elde edilmiştir.

Ortalama paket boyutu: Bir saniyede iletilen tüm paketlerin, Byte cinsinden uzunluklarının (başlık ve yararlı yük dahil) toplamının saniyede gelen paket sayısına bölünmesi ile elde edilir. Bu öznitelik TCP SYN baskını saldırısı gibi yüksek sayıda küçük paketler üreten trafiğin tespitinde kullanılabilir.

Toplam Paket Sayısı: Bir saniyede ağ trafiğinde bulunan paketlerin toplam sayısıdır.

SYN, RST, ACK Paket Sayısı: Bir saniyede gelen toplam TCP paketlerinden bayrak bitlerine göre ayrılmış sayılarıdır. Bu bayrak bitleri paketin cinsine göre değişmektedir.

TCP Paket Sayısı: Bir saniyede gelen toplam TCP paketlerinden sayısıdır.
Tüm paketlerin sayısı: Bir saniyede gelen toplam paketlerin sayısıdır.

UDP Paket Sayısı: Saniyede gelen UDP paket sayısıdır. TCP SYN flood saldırısını engellememesi beklenmektedir ancak öznitelik seçiminde etkisi incelenmiştir.

ICMP Paket Sayısı: Saniyede gelen ICMP paket sayısıdır.

Benzersiz IP sayısı: Saniyede ağ trafiğinde bulunan paketlerinin kaynak IP'lerinin benzersiz olanlarının sayısıdır.

Benzersiz akış sayısı: Bir saniyede ağ trafiğinde bulunan paketlerin kaynak ve hedef IP çiftlerinin benzersiz olanlarının sayısıdır.

DETER test ortamında [6] oluşturulan saldırı ve normal trafik benzetimlerinde yukarıda bahsedilen trafik öznitelikleri incelenmiştir.

TCP SYN baskını saldırılarını içeren veride, trafikteki ortalama paket boyutu özniteliğinin, diğer öznitelikler ile ters ilintili olduğu görülmüştür. Saldırı anında pek çok küçük boyutlu paket üretilmesi, ortalama paket boyunun azalmasına sebep olurken, diğer öznitelikler artmaktadır. Bu durum saldırı anında bu özniteliklerin ters ilintili olmasını sağlamaktadır. Oluşturacağımız saldırı tespit mekanizmasında kullandığımız ilinti katsayı matrisi, yönteme öznitelikler arasındaki bu ilişkiyi eklemektedir.Bu amaçla, özbağlanımlı süreç ve bu süreç sonucu elde edilen trafik sağlık fonksiyonu [7] kullanılmıştır.

4.1Bilgi Kazancı ile Öznitelik Seçimi

Bu çalışmada DDoS tespiti için zaman serilerinde ani değişikliklere bakıldığından saldırı tipi ile ilgili olmayan özniteliklerdeki değişiklikler yanlış alarmlara sebep olabilirler. Bu sebepten 9 öznitelikten TCP SYN baskını saldırıları ile ilgili en fazla bilgi içeren özniteliklerin seçilmesi sistem performansını ve sonuçları etkileyecektir.

Saldırı çeşidine göre ayırt edici özniteliklerin seçimi için bilgi kazancı (ing:informaiton gain) yöntemi kullanılmıştır. Temel olarak bilgi kazancı, söz konusu özniteliğin saldırı olup olmadığı ile ilgili verdiği bilgi kalitesidir [8].

Bilgi kazancını hesaplamak için öncelikle etiketlenmiş bir zaman serisinin olması gereklidir. Bunun için ağda bulunan paketler hedef IP adreslerine göre filtrelenip, hedef bilgisayarın IP adresi olan paketler saldırı paketleri olarak etiketlenir.

Trafik öznitelikleri bir saniye aralığında hesaplandığından, etiketlenmiş zaman serisi belirlenen saniyede saldırı olup olmadığı bilgisini bize sağlamaktadır. Özniteliğin herhangi bir elemanının bulunduğu saniyede saldırı paketi var ise o eleman saldırı olarak etiketlenir.

Etiketler şu şekilde düzenlenir ise: 0 saldırı yok, 1 saldırı var. Bilgi kazancının en yüksek seviyesi yani öznitelikten beklenen bilgi miktarı hesaplanabilir.

$$I(s_1 s_2) = -\sum_{i=1}^{2} \frac{s_i}{s} \log_2\left(\frac{s_i}{s}\right). \qquad (4)$$

Burada s_1 guruba ait örnek sayısı iken s_2 guruba ait olmayan örnek sayısıdır. Eğer bütün örnekler gurubun içinde veya gurubun dışında ise beklenen bilgi sıfırdır. Bu durumda bütün özniteliklerin bilgi kazancı sıfıra eşit olur ve özniteliği saldırı olup olmadığı konusunda incelemek gereksizdir. Diğer taraftan örneklerin yarısı guruba aitken yarısı değil ise bilgi kazancı 1 e eşit olur ve bu öznitelikler sınıflandırma için en önemli öznitelikler olarak seçilirler.

Bir özniteliğin bilgi kazancını hesaplamak için öncelikle özniteliğin her sınıf için ayrı ayrı entropisi hesaplanır. Bu değer etiket serisinin beklenen bilgi değerinden çıkarılır. Örneğin F={f1, f2, … fr} özniteliğinin entropisi şu şekilde hesaplanır.

$$E(F) = \sum_{i=1}^{r2} \frac{s_{1i}+s_{2i}}{s} I(s_{1i}, s_{2i}). \qquad (5)$$

Burada s_{1i}, öznitelikteki örneklerin i sınıfına ait olanlarının sayısıdır. Yani öznitelikteki bir örnek, bulunduğu zamanda saldırı olup olmamasına göre sınıflanır. Bir özniteliğin bilgi kazancı:

$$Gain(F) = I(s_1, s_2) - E(F). \qquad (6)$$

Tablo 2. 9 Öznitelik için DETER test ortamında birinci deney için hesaplanan bilgi kazancı.

Öznitelik	**Bilgi Kazancı**
Benzersiz Akış Sayısı	0.762
RST Paket Sayısı	0.724
Benzersiz IP Sayısı	0.722
SYN Paketi Sayısı	0.620
TCP Paketi sSayısı	0.596
Toplam Paket Sayısı	0.595
ACK Paketi Sayısı	0.413
ICMP Paketi Sayısı	0.355
UDP Paketi Sayısı	0

Tablo 1 de DETER test ortamında yapılan benzetimlerden birincisi için hesaplanan bilgi kazancı gösterilmektedir. Yapılan diğer benzetimler için de benzer sonuçlar elde edildiğinden burada gösterilmemiştir.

Bilgi kazancı hesaplamasına göre TCP SYN baskını saldırıları için ilk 4 öznitelik seçilmiş ve sonuçlar sonraki bölümde paylaşılmıştır.

5.Benzetimler

Bu bölümde, DETER test ortamında yapılan TCP SYN baskını saldırı benzetimleri hakkında özet bilgi yer almaktadır. Test ortamında, DETER laboratuarları tarafından sağlanan SEER ara yüzü kullanılarak saldırı içermeyen arka plan trafiğin yanında, TCP SYN baskını saldırıları ile ilgili benzetimler yapılmıştır. Bu benzetimlerde farklı oranlarda saldırı ve arka plan trafiği kullanılmıştır.

Bu benzetimler hem saldırı hem de normal trafiği aynı anda barındırmaktadırlar. Bu benzetimlerden elde edilen trafik öznitelik dizileri için sağlık fonksiyonu hesaplanmış ve bu fonksiyonlar eşiklenerek uyarılar üretilmiştir. Bu uyarılar, saldırıların başlangıç ve bitiş zamanlarında ortaya çıkmaktadır.

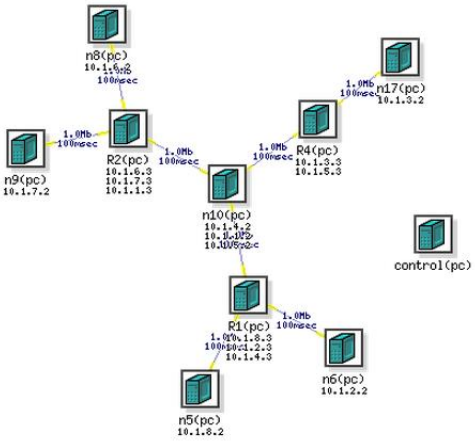
Bu bildiri, yapılan bütün benzetimlerin ayrıntılarını içermemektedir. Bunun yerine kullanılan yöntem, çeşitli oranlarda ve sürelerde 9 adet saldırı içeren bir benzetim ile açıklanmıştır.

5.1.TCP SYN Baskını Saldırısı Benzetimi

Bu benzetim 15 dakika süren arka plan trafiğinin yanı sıra, 9 adet, farklı zamanda oluşturulan TCP SYN baskını saldırısı içermektedir.

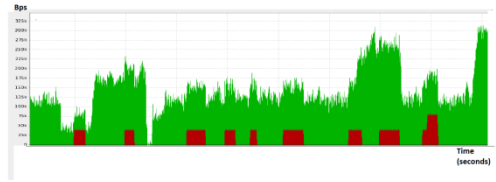
Benzetimler için bir hedef bilgisayar bir sunucu bilgisayar ve 7 adet istemci ve saldırgan bilgisayar kullanılmıştır. Saldırıların DDoS olabilmesi için saldırganlar gönderdikleri saldırı paketlerinin kaynak IP adresleri yerine sahte IP adresleri kullanmışlardır. Üretilen DDoS paketleri 1024 farklı kaynak IP adresi içermektedir. Benzetimler için kullanılan ağ topolojisi şekil 2 de gösterilmiştir.

Deney topolojisinde N9 hedef bilgisayardır ve herhangi bir trafik yapmamaktadır. N9 bilgisayarı herhangi bir ağ trafiği yapmamaktadır, sadece saldırıları karşılamaktadır. Ağ trafiğinden alınan paketlerden hedef IP adresi N9 olanlar saldırı paketi olarak etiketlenmiştir. Bu etiketler kullanılarak ağdan yakalanan paketler saldırı ve normal olarak iki ayrı sınıfa ayrılmıştır. Bu etiketler bilgi kazancını hesaplamak için kullanılmıştır.



Şekil 2. DETER test ortamında benzetimler için oluşturulan ağ topolojisi.

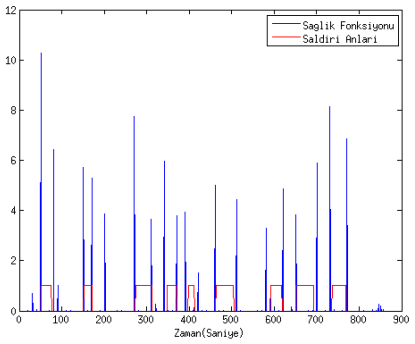
DETER test ortamında benzetimler yapılırken farklı trafik oluşturma araçları tanımlanabilmektedir. Deneylerde çeşitli istemcilerden gelen SSH, DNS, paket tekrarlayıcı, web, FTP gibi arka plan trafikleri oluşturulabilmektedir. Şekil 3 de görüleceği üzere farklı trafik oluşturma araçları kullanarak değişken arka plan trafiği oluşturulmuştur. Burada saldırı içermeyen ancak yoğunluğu zamanla değişen paketlerin önerilen DDoS tespit yöntemine etkisi olmadığını şekil 4 de gösterilen ağ trafiği sağlık fonksiyonun da görmekteyiz.



Şekil 3. Birinci Deneyin trafik grafiği (Bps/Zaman). Kırmızı ile gösterilen yerler

saldırının oluşturduğu paketlerin saniyedeki bit sayısıdır.

Şekil 4'de bu benzetim için hesaplanan trafik sağlık fonksiyonu ile 9 adet saldırının başlangıç ve bitiş noktaları gösterilmiştir. Burada eşikleme için herhangi bir yöntem kullanılmamıştır. Yanlış alarm sayısını arttırmadan bütün saldırıların tespitini sağlayan en uygun eşik değeri olan 3.7 değeri, deneysel olarak belirlenmiştir.



Şekil 4. Birinci benzetim için hesaplanan ağ trafik sağlık fonksiyonu (mavi) ve saldırı zamanları (kırmızı).

Sonuçlar ve Öneriler

Bu bölümde, saldırı içeren 3 adet benzetimde hesaplanan trafik sağlık fonksiyonunun eşiklenmesi ile oluşturulan alarmların değerlendirilmesi yapılmaktadır (Tablo 2).

Bu bölümde, saldırı içeren 4 adet benzetimde hesaplanan trafik sağlık fonksiyonunun eşiklenmesi ile oluşturulan alarmların değerlendirilmesi yapılmaktadır.

Testler kapsamında, birincisi önceki bölümde detaylı olarak gösterilen deney olmak kaydıyla, 4 adet saldırı içeren deney yapılmıştır. Bu deneyler yaklaşık 15 dakika süresince yapılan çeşitli arka plan ve saldırı trafiklerini içermektedir. Bunlardan ilki 9 adet TCP SYN baskını saldırısı içermektedir. Benzetim sonucunda elde edilen özniteliklerden hesaplanan sağlık fonksiyonu kullanılarak; 18 farklı noktanın tespit edilmesi beklenmektedir.

Tablo 2 de görüleceği üzere ilk deney için sadece 3 yanlış alarm ile bütün saldırıların başlangıç ve bitiş noktaları tespit edilebilmiştir. Benzer bir şekilde ikinci deneyde 6 adet saldırıya ait 12 adet başlangıç ve bitiş noktasından biri dışında bütün saldırılar tespit edilebilmiştir. Son deneyse ise yanlış alarm olmadan 5 adet saldırının başlangıç ve bitiş noktaları tespit edilebilmiştir.

Tablo 2. Dört farklı deneyde ağ sağlık fonksiyonunun eşiklenmesi sonucunda elde edilen alarmlar ve değerlendirmesi.

Deney	Saldırı Sayısı	Doğru Alarm	Yanlış Alarm
1	9	18	3
2	6	11	1
3	5	10	0
4	6	12	1

Bu sonuçların çeşitliliği, arka plan trafiğindeki değişimlere ve saldırı trafiği ile arka plan trafiği arasındaki orana bağlıdır. Farklı arka plan trafiği ve saldırı trafiği oranlarında farklı sonuçlar elde edilebilmektedir.

Bu çalışma DETER test ortamı ile yapılan deneylere dayanmaktadır. Elde edilen trafik 9 farklı öznitelikten 4 ayrı trafik özniteliği seçilmiştir incelenmiştir.

Kaynaklar

[1] Abbass Asosheh and Naghmeh Ramezani, "A Comprehensive Taxonomy of DDoS Attacks and Defense Mechanism Applying in a Smart Classification", **WSEAS Transactions on Computers**, 7(4):281–290, 2008.

[2] Jelena Mirkovic and Peter Reiher, "A taxonomy of ddos attack and ddos defense

mechanisms.", **SIGCOMM Comput. Commun. Rev**., 34:39–53, 2004.

[3] M Thottan and Chuanyi Ji Chuanyi Ji, "Anomaly detection in ip networks.", **IEEE Transactions on Signal Processing**, 51(8):2191–2204, 2003.

[4] M Thottan and Chuanyi Ji Chuanyi Ji, "Adaptive thresholding for proactive network problem detection.", **Proceedings of the IEEE Third International Workshop on Systems Management**, pages 108–116, 1998.

[5] Umut Güven, "A combined wavelet and autoregressive based statistical intrusion detection system.", **Master's thesis**, Boğaziçi Üniversitesi, 2007.

[6] Terry Benzel, Robert Braden, Dongho Kim, Clifford Neuman, Anthony Joseph, Keith Sklower, Ron Ostrenga, and Stephen Schwab, "Design, deployment, and use of the deter testbed.", **In Proceedings of the DETER Community Workshop on Cyber Security Experimentation and Test**, pages 1–1, Berkeley, CA, USA, 2007.

[7] M Thottan and C Ji, "Fault prediction at the network layer using intelligent agents.", **Integrated Network Management VI Distributed Management for the Networked Millennium Proceedings of the Sixth IFIPIEEE International Symposium on Integrated Network Management,**Cat No99EX302, pages 745–759, 1999.

[7] Harry L Van Trees., "Detection , Estimation , and Modulation Theory, volume 6.", **John Wiley & Sons, Inc.,** 2001.

[8] Kayacık, H.G., A.N. Zincir, M.I. Heywood, "Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Dataset", **Proceedings of the Third Annual Conference on Privacy, Security and Trust**, St. Andrews, NB, Canada, 2005.1