İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

AĞ TRAFİĞİNİN ANALİZİ, ANOMALİ TESPİTİ VE DEĞERLENDİRME

YÜKSEK LİSANS TEZİ

Akın ASLAN

Bilişim Uygulamaları Anabilim Dalı

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

ARALIK 2017

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

AĞ TRAFİĞİNİN ANALİZİ, ANOMALİ TESPİTİ VE DEĞERLENDİRME

YÜKSEK LİSANS TEZİ

Akın ASLAN
(707151003)

Bilişim Uygulamaları Anabilim Dalı

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

Tez Danışmanı: Doç. Dr. Enver ÖZDEMİR

ARALIK 2017

İTÜ, Bilişim Enstitüsü'nün 707151003 numaralı Yüksek Lisans Öğrencisi Akın ASLAN, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "AĞ TRAFİĞİNİN ANALİZİ, ANOMALİ TESPİTİ VE DEĞERLENDİRME" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Doç. Dr. Enver ÖZDEMİR** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Doç. Dr. M.Oğuzhan KÜLEKCİ** İstanbul Teknik Üniversitesi	.....
	Yrd. Doç. Dr. Erdinç ÖZTÜRK Sabancı Üniversitesi	.....

Teslim Tarihi : 17 Kasım 2017
Savunma Tarihi : 21 Aralık 2017

Oğluma,

ÖNSÖZ

Bu tez çalışmasının planlanmasında, araştırılmasında ve oluşumunda ilgi ve desteğini esirgemeyen, bilgi ve tecrübelerinden yararlandığım, çalışmamı bilimsel temeller ışığında şekillendiren sayın hocam Doç. Dr. Enver ÖZDEMİR'e sonsuz teşekkürlerimi sunarım.

Kasım 2017 Akın ASLAN

İÇİNDEKİLER

Sayfa

KISALTMALAR

ANN : Artificial Neural Network
ARP : Address Resolution Protocol
CIDF : Common Intrusion Detection Framework
CIS : Communication and Information Systems
DARPA : Defense Advanced Research Projects Agency
DDOS : Distributed DOS
DNS : Domain Name System
DOS : Denial of Service
EMA : Exponential Moving Average
FANN : Fast Artificial Neural Network
FN : False Negative
FP : False Positive
GNU : GNU's Not UNIX
HMA : Hull Moving Average
HTML : Hypertext Markup Language
HTTP/S : Secure Hypertext Transfer Protocol
ICMP : Internet Control Message Protocol
IDE : Integrated Development Environment
IDMEF : Intrusion Detection MEssage Format
IDS : Intrusion Detection Systems
IDXP : Intrusion Detection eXchange Protocol
IETF : Internet Engineering Task Force
IIS : Internet Information Services
IP : Internet Protocol
MySQL : My Structured Query Language
RARP : Reverse Address Resolution Protocol
PCAP : Packet Capture
RoC : Rate of Change
SMA : Simple Moving Average
SMTP : Simple Mail Transfer Protocol

STA **:** Situation Transition Analysis

SYN **:** synchronize

TCP **:** Transmission Control Protocol

TN **:** True Negative

TP **:** True Positive

TTL **:** Time to Live

UDP **:** User Datagram Protocol

WMA **:** Weighted Moving Average

XML **:** Extensible Markup Language

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

AĞ TRAFİĞİNİN ANALİZİ, ANOMALİ TESPİTİ VE DEĞERLENDİRME

ÖZET

Bilgisayar ağlarının dünya çapında yaygın olarak kullanılmasıyla, ihtiyaç duyulan her yerden bilgiye anında erişmek, işlemek ve paylaşmak daha önce hiç olmadığı kadar kolay olmuştur. Bilgisayar ağları her geçen gün artan işlem kapasiteleri yardımıyla bilgiyi daha kullanışlı hale getirerek dünya genelinde bilgiyi her an erişilebilir kılmışlardır. Dünya çapında her yerden erişilebilir olan ve günden güne genişleyen İnternet, bilgisayar ağlarının en önemli örneğidir. İnternet dünya üzerinde iletişime, bilgi paylaşımına, devletler ve özel kurumlar gibi hizmet sağlayanlara önemli bir altyapı olmuştur. Bilgisayarların ve İnternetin getirdiği söz konusu kolaylıklar sayesinde bilgisayar ağlarının önemi her gün artmakta, çevrim içi İnternet hizmetleri ve kullanıcı sayıları sürekli artış göstermektedir.

Kurum ve kuruluşlar, hizmet kalitesini ve çeşitliliğini artırmak için kullanıcılardan elde ettikleri muazzam miktarda ki veriyi işlemek zorundadırlar. Verilerin toplanması ve işlenmesi çoğu zaman bilgisayar ağları ile birbirine bağlı farklı bilgisayar sistemleri üzerinde gerçekleşmektedir. Bunun sonucu olarak elde edilen büyük miktarlarda ki veri farklı yerlerde saklanmak zorunda kalınmaktadır. Veri işleyen ve saklayan sistemlerin İnternet altyapısı ile belirlenmiş sınırlar içinde kullanıcıların erişimine açık kalmaktadır. Bunun getirmiş olduğu kolaylıkların yanında, kurum ve kuruluşlara çeşitli nedenlerle zarar vermek isteyenler için bilgisayar ağları ile veri ve hizmet sunan sistemler öncelikli hedefler arasında yer almaktadır.

Siber güvenlik konusuna ilgi duymayanların bile artık haberdar olduğu üzere siber uzayda icra edilen saldırıların sonucunda hizmet sunan sistemlere erişimde büyük ölçekte kesintiler oluşmakta, veri kayıpları yaşanmakta, ileri seviyede gerçekleşen başarılı ve yıkıcı saldırılar ile büyük maddi zararların oluşmasının yanında kurum ve kuruluşların güvenilirliği ve itibarı azalmaktadır. İlaveten, siber saldırganlar her geçen gün yeni yöntemler keşfetmekte ve bilgisayar ağları üzerindeki faaliyetlerinin tespiti her geçen gün daha zor hale gelmektedir. Bilgisayar ağlarının korunması ve siber saldırganların faaliyetlerinin belirlenmesi için bilgisayarların ve ağların üstünde çalışmak üzere tasarlanan güvenlik sistemleri mevcuttur. Saldırı Tespit Sistemi adı verilen güvenlik sistemleri artan güvenlik endişelerine paralel olarak gelişmeye devam etmektedirler. Siber saldırganların keşfettikleri yeni yöntemlerin tespit edilebilmesi için Saldırı Tespit Sistemlerinin bir ağdaki anomalileri tespit edebilecek seviyede tasarlanmaları gerekir. Bu sistemlerin uyguladığı ağ trafik analizinde temel yaklaşım şüpheli trafiğin tespit edilmesi ve normal trafikten ayrılmasıdır.

Saldırı Tespit Sistemlerinin tasarlanmasında ortak bir standart oluşturmak için The Internet Engineering Task Force (IETF) tarafından genel bir Saldırı Tespit Sistemi çerçevesi oluşturulmuştur. Belirlenen standartlar ile Saldırı Tespit Sistemleri aralarında veri paylaşmaları ve gerektiğinde de beraber çalışmaları mümkün olmuştur.

Bu kapsamda tasarlanan ve üretilen sistemlerin doğru bir şekilde karşılaştırması da yapılabilmektedir. Karşılaştırmada kullanılmak üzere birçok ölçüt önerilmiştir. En önemlileri arasında Tespit Oranı ve Yanlış Alarm Oranı vardır. Ağ üzerindeki tüm verinin sürekli analiz edilmesi sistem üstünde fazladan yük yaratacaktır. Analiz edilmesi gereken tüm veriler aynı önem derecesine sahip olmadıkları için mevcut Saldırı Tespit Sistemi çerçevesine ilave olarak risk değerlendirmesi yapan bir bloğun eklenmesi ve analiz bloğunu yönlendirmesi verimliliği arttıracaktır.

Bilginin güvence altına alınmasında fiziki ve personel güvenliğinin yanında Saldırı Tespit Sistemleri de kullanılmalıdır. Saldırı Tespit Sistemleri ile temel olarak bilginin bütünlüğü, gizliliği ve erişilebilir olması korunmaktadır. Teknik olarak bunu yaparken farklı tespit yaklaşımları kullanılmaktadır. Tespit yaklaşımları İstatistik Tabanlı, Bilgi Tabanlı ve Makine Öğrenme Tabanlı olmak üzere 3 ana başlık altında değerlendirilmiştir. İstatistik Tabanlı tespit sisteminde "normal" olarak kabul edilen veri trafiği izlenerek olasılıklara dayalı bir istatistiksel model oluşturur. Olağan dışı olaylardan şüphelenilmesi gerektiği için, model dışında kalan olaylarda Saldırı Tespit Sistemleri uyarılarda bulunmaktadır. Bilgi Tabanlı yaklaşım Saldırı Tespit Sistemlerinde yaygın olarak kullanılmaktadır. Yaklaşımın uygulanmasında korunan bilgisayar sistemi ve ağı hakkında çeşitli yöntemlerle kurallar oluşturulur. Benzer şekilde kural ihlalinde uyarı oluşturulmaktadır. Makine Öğrenme Tabanlı yaklaşım da yapay zekâ uygulamaları öne çıkmaktadır. Çok karışık veri kümelerinin analizinde çok başarılı sonuçlar üreten bir yaklaşım olsa da bilgisayar sistemlerine çok daha fazla işlem yükü getirmektedirler.

Saldırı Tespit Sistemi tasarımında en dikkatli tasarlanması gereken bölüm analizden sorumlu olan bloktur. Tespit etme yaklaşımlarının uygulandığı analiz bloğunun performansı doğrudan doğruya Saldırı Tespit Sisteminin başarımını belirleyecektir. Her bir tespit yaklaşımı ayrı ayrı incelendiğinde birbirlerine göre üstün yönleri olduğu görülmektedir. Fakat hiçbirisi tüm yönleri ile bir diğerinden üstün değildir. Tek bir yaklaşım ile tasarlanan bir sistemin koruma kabiliyetinin eksik kalacağı anlaşılmaktadır. Bu maksatla en az iki farklı yaklaşıma ait ikiden fazla yöntemin bir arada kullanılması verimli bir tespit etme olanağı sağlayacaktır. Tez çalışmasında anormallik yaratan durumların tespit edilebilmesi için bilgisayar sistemine yönelik saldırıların ayak izlerine bakarak anomalileri keşfetmek için bir dizi yeni tespit yöntemi önerilmiştir. Bilgi Tabanlı Analiz ile İstatistik Tabanlı Analiz bir arada düşünülmüştür. Doğrusal olmayan zaman serileri ile modellemesi yapılan ağ trafiği içinde tespit edilen anormallikler şüpheli olarak etiketlenmişlerdir.

Siber saldırılar arasında en büyük oranda verilen hizmetlerin durdurulmasını veya yavaşlatılmasını amaçlayan Hizmet Reddi (DOS) saldırısı ve türevleri yer almaktadır. Önerilen tespit sistemi içinde bir DOS saldırısı veya türevinin saldırı başında oluşturması muhtemel anormallikleri tespit etmeye yönelik analiz yöntemleri açıklanmış ve uygulamalarla ilk testleri yapılmıştır. Saldırı hazırlığında olan kötü niyetli bir kişi, eylemlerinin tespit edilmemesi için karşı tedbir olarak öğrenme kabiliyetine sahip sistemleri istediği yönde eğitmeye başlayacaktır. Önerilen hibrid tespit sisteminin istenen yönde eğitilmemesi için tespit yaklaşımlarını destekleyici bir yöntem daha belirlenerek önerilen tespit sistemi içinde test edilmiştir.

Sonuç olarak bilgisayar ağları üzerinde meydana gelen saldırılardan korunmak ve mümkün olduğunca durdurabilmek için, gelişimleri hızla devam eden Saldırı Tespit Sistemlerinin kullanılması bilginin güvenceye alınmasında önemli olduğu değerlendirilmiştir.

ANALYSIS OF NETWORK TRAFFIC, ANOMALY DETECTION AND EVALUATION

SUMMARY

With the available computer networks worldwide, it has never been easier to access, process and share information instantaneously wherever it is needed. The computer networks makes knowledge more useful and worldwide accessible at all times with the help of ever increasing processing capacities. The Internet, which is accessible all over the world and is expanding day by day, is the most important example of computer networks. The Internet has become an important infrastructure for communication, information sharing, and service providers such as governments and private institutions. The convenience that computers and Internet brought has increased the number of online Internet services and number of users who has of these services.

Institutions and organizations have to deal with the tremendous amount of data they get from users to increase the quality and diversity of services. The collection and processing of data often takes place on different computer systems interconnected by computer networks. As a result, large amounts of data are required to be stored in different locations. With the Internet infrastructure, systems that process and store data remains available to users within specified limits. Besides these conveniences, computer networks and systems providing data and services are among the priority targets for those who want to harm institutions and organizations for various reasons.

As even those who are not interested in cyber security are now aware that successful and destructive advanced level of cyber space attacks have resulted in massive interruptions in access to the systems that provide service, resulting in data loss, and major financial losses, as well as decreasing credibility and reputation of institutions and organizations. In addition, cyber attackers are discovering new methods every day and the detection of their activity on computer networks is becoming more and more difficult every day.

There are security systems designed to work on computers and networks for the protection of computer networks and for the identification of cyber attackers' activities. Security systems, called Intrusion Detection Systems, continue to evolve in parallel with increased security concerns. In order to detect new methods discovered by cyber attackers, Intrusion Detection Systems must be designed at a level that can detect anomalies in a network. The basic approach in network traffic analysis is to detect suspicious traffic and to distinguish it from normal traffic.

The Internet Engineering Task Force (IETF) established a framework to establish a common standard in the design and production of Intrusion Detection Systems. With established standards, Intrusion Detection Systems are able to share data among themselves and work together when necessary. In this context, it is possible to compare the produced systems correctly. Many criteria have been proposed for use in comparison. The most important ones are Detection Rate and False Alarm Rate.

Continuous analysis of all data on the network will create an extra load on the system. Since not all the data to be analyzed have the same significance, adding a risk assessment block in addition to the existing Intrusion Detection System framework and directing the analysis block will increase the efficiency. The value of the protected data should be used as a basic input for a risk analysis. It is also necessary to determine how much of the risks can be accepted and how much can be mitigated. The crucial question here is “how to mitigate the risks”.

In order to secure information, Intrusion Detection Systems (IDS) should be used besides the physical and personnel safety precautions. Intrusion Detection Systems basically protect the integrity, confidentiality and accessibility of information. Technically, they use different detection approaches when doing this. The detection approaches are evaluated under 3 main topics as Statistics Based, Knowledge Based and Machine Learning Based.

In the Statistical Based, the IDS follows the "normal" network activity and builds a statistical model, a pattern of it. A behavioral model is created based on the probabilities for each event by observing network traffic. And then any traffic outside the normal range is simply marked as anomaly. Because unusual events are suspicious in terms of security. Finally the Intrusion Detection System alerts for the events which are outside the model. Knowledge-based approach is widely used in Intrusion Detection Systems. In the implementation of the approach, rules are established with various methods about the protected computer system and network. Similarly, a warning is generated in violation of the rule. Artificial intelligence applications come to the forefront in Machine Learning Based Approach. Although it is an approach that produces very successful results in the analysis of highly complex data clusters, it introduces much more computational burden to computer systems.

The most carefully designed part of an Intrusion Detection System framework is the block responsible for the analysis. The performance of the analysis block, where detection approaches are applied, will directly determine the performance of the Intrusion Detection System. When each detection approach is examined separately, it is seen that they have advantages over each other. But none, in all its aspects, is superior to another. It is understood that the protection capability of a system designed with a single approach will be insufficient.

For this purpose, a combination of two or more methods of at least two different approaches will provide an efficient detection. A number of new detection methods have been proposed to detect the anomalies in the thesis work by looking at the footsteps of the attacks on the computer system. Knowledge Based Analysis and Statistical Based Analysis are considered together. The anomalies detected in the network traffic modeled with non-linear time series are labeled as suspicious.

Today, it is very important to provide a high level of security to ensure that information is securely and reliably stored and transferred. However, secure communication over the Internet or any other network is always under threat of intruders and their activities are any set of actions that try to put the integrity, confidentiality, availability of the information at risk. Among the cyber attacks, the most common type of attack is the Denial of Service (DOS) and its variants, which aim to stop or slow down the services. In the proposed detection system, selected methods of analysis for detecting possible anomalies of early phase of DOS attacks or derivatives have been described and initial tests have been carried out with the applications.

While trying to produce realistic results, it should always be known that the noise is also present in the system, which can lead to false alarms. This is very important issue that needs to be taken into consideration. Thresholds values used in the analysis block determine how far the system will perceive the noise as a real alarm, and how much the real anomalies will look normal.

The IDS industry appears to be rapidly becoming a growing sector. Among the many criticisms about IDS are their performances and prices, an important component that determines the price of an IDS is how much network traffic can be captured. No matter how good a method of analysis is used, it is not possible to be certain that information security is precise unless the network traffic is thoroughly watched.

IDSs are now the indispensable main element of security systems. They are rapidly evolving, and considered to be the most important technical issue in securing information in order to protect against possible attacks on computer networks and to stop as much as possible. However, most IDS produced contain commonly accepted detection methods. The novel approaches described in this thesis in terms of shedding light on the work to be done in the future offer considerable features in terms of practicality and operation. It is now possible to capture normal patterns and find anomaly ones even in mixed environments of normal and anomaly traffics.

1. GİRİŞ

Günümüz dünyası "Bilgi" açısından çok zengindir ve her alanda bilgisayarlar bilginin işlenmesi, iletilmesi ve saklanması için vazgeçilmez birer araç olmuşlardır. Bilgisayarların bu yetenekleri, aralarında veri alış verişi yapabilmelerine olanak sağlayan bilgisayar ağları ile desteklenmektedir. Bir bilgisayar ağı bilginin dâhil olduğu yazılım ve donanım kaynaklarının paylaşılması için birden fazla bilgisayarın birbirine bağlandıkları bir sistemdir.

Bilgisayar ağı kavramı bilgisayarların fiziksel bağlantılarından üzerlerinde çalışan uygulamaların iletişim kanallarına kadar olan birden fazla katmanın bir araya gelmesi ile açıklanabilir. Her katmanın belirli bir görevi vardır ve diğer tüm katmanlardan bağımsız olmalarına rağmen bir bütün olarak çalışırlar. Bilgisayar ağı ile bilgisayar arasında gelen ve giden veriler sırasıyla her bir katmandan geçerek iletilirler.

Katmanlı bir iletişim mimarisi oluşturmak için bilişim dünyasına birden fazla model tanıtılmış ve uygulanmıştır. Önemli olanlar arasında genel haberleşme için kullanılan 7 katmanlı OSI [37] modeli ve İnternet iletişimi için özelleştirilmiş olan 4 katmanlı Internet Model [38] bulunmaktadır. Internet Model sırasıyla Bağlantı, İnternet, Ulaştırma ve Uygulama (Link, Internet, Transport, Application) katmanlarından oluşmaktadır. Bağlantı katmanı belirli iletişim kurallarına (Ethernet, ARP vb.) göre ağ kartından gelen verileri İnternet katmanına taşımaktan sorumludur. İnternet katmanında gelen paketlerin IP adresleri bulunmaktadır. Aynı zamanda İnternet bağlantısının kontrol edilmesi için kullanılan ICMP paketleri de bu katmanda bulunur. IP adresine göre yönlendirilen paketler Ulaştırma katmanına gönderilirler. Burada her bir paket ait oldukları protokole (TCP, UDP vb.) göre bir kez daha ayrılırlar. İlgili protokole göre ayrılan paketler son katman olan Uygulama katmanına ulaşarak port numaralarına (80:HTTP, 21:FTP vb.) göre kullanılacakları uygulamalara taşınırlar.

Bilgisayar ağlarının muazzam gelişimi ve bunları kullanan uygulamaların sayısındaki hızlı artış nedeniyle ağ güvenliği giderek daha fazla önem kazanmaktadır. Dahası, neredeyse tüm bilgisayar sistemleri, teknik açıdan tespit edilmesi zor olan ve önlenmesi maliyetli olan güvenlik açıklarına sahiptir. İnternet Modelin içinde yer alan IP, TCP gibi protokollerin de güvenlik önlemleri olmadan ağ iletişiminin kusursuz bir şekilde yapılabilmesi için tasarlanmış olmaları da güvenlik açıklarının oluşmasına katkı sağlamaktadır.

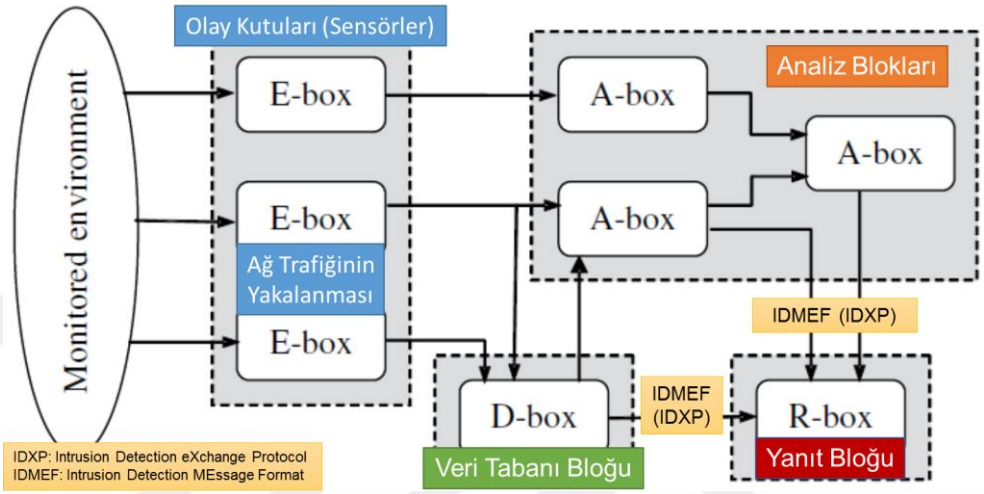
Bu nedenle, bir ağdaki anomalileri ve saldırıları tespit etmek için tasarlanan, en önemli ağ güvenlik elemanı olan Saldırı Tespit Sistemleri (IDS) daha da önem kazanmaktadır. Bu sistemlerin uyguladığı ağ trafik analizinde temel yaklaşımlardan biri, şüpheli trafiği tespit etmek ve normal trafikten ayırmaktır. Bunu yapabilmek için ise imza tabanlı, bilgi tabanlı ve makine öğrenmeyi temel alan çeşitli yöntemler geliştirilmiştir [1].

Günümüzün İnternet ortamında, farklı işlem gücü olan sayısız taşınabilir bilgisayar özellikleri olan aygıtlar bulunmaktadır. Özellikle konu taşınabilir olduğunda yüksek işlem gücü ve performansı kısıtlayan anormallik tespit çözümlerinin çok daha az tercih edileceği açıktır [2].

1.1 IDS Konsepti

Saldırı Tespit Sistemi (IDS), İletişim ve Bilgi Sistemlerinin (CIS) genel güvenliğini diğer güvenlik araçları gibi daha da güçlendirmeyi amaçlayan bir bilgisayar / bilgisayar ağı güvenlik aracıdır [3]. Günümüze kadar pek çok farklı IDS yaklaşımı [4,5] sunulmuş ve bunların neredeyse tamamı The Defense Advanced Research Projects Agency (DARPA) tarafından tanımlanan ortak bir çerçeveye sahiptir. Bu kapsamda her türlü IDS için tanımlanan ortak yapının koordine edilmesi ve detaylarının ortaya konması için DARPA tarafından desteklenen araştırmacılardan oluşturulan The Internet Engineering Task Force (IETF) görevlendirilmiştir [1]. Bu çalışmaların sonucu olarak temel özellikleri belirlenmiş olan Genel Saldırı Tespit Çerçevesi (CIDF) [6] donanım geliştiricilerine, üreticilerine ve bilgi sistem uzmanlarına tanıtılmıştır. Tasarlanan CIDF içeriği Şekil 1.1'de sunulmuştur.

CIDF'nin temel amacı, birçok IDS'in mümkün olduğunca elde ettikleri verileri aralarında paylaşabilmelerini ve gerektiğinde de beraber çalışmalarını sağlayacak olan bir dizi teknik özellikler bütününü belirlemektir. Ayrıca, bir IDS'in sahip olduğu modüllerin asıl tasarlandıkları amaçlarından farklı alanlarda da kullanılmasını mümkün kılmaktır [6]. IDS'lerin sahip olduğu veri tabanı yönetim sistemleri, analiz metotları aynı zamanda iyi birer veri madenciliği aracı olarak da kullanılmaktadır.



Şekil 1.1 : Genel Saldırı Tespit Çerçevesi (CIDF).

CIDF konseptinde dört farklı işlev alanı bulunmaktadır. Bunlar, sensör bloğu (E), analiz bloğu (A), veri tabanı bloğu (D) ve yanıt bloğudur (R). Sensör bloğu, hedef sistemi izleyen ve analiz bloğu tarafından analiz edilecek bilgileri elde eden sensör öğelerinden oluşmaktadır. Analiz bloğu, sensörler tarafından yakalanan olayları analiz eder ve potansiyel düşmanca davranışları tanımlar. Olası bir tehdit veya bir saldırı tespit ettiğinde yanıt bloğunu tetikler ve sistem yöneticilerini uyarmak için bir alarm oluşturur. Ayrıca aldığı tüm bilgileri kaydedilmesi için veri tabanı bloğuna gönderir. Yanıt bloğu, analiz bloğu tarafından tanımlanan herhangi bir saldırıyı önlemeye yönelik eylemleri gerçekleştirmek üzere tasarlanmıştır. Son olarak ise veri tabanı bloğu, sensör ve analiz blokları tarafından bir araya getirilen tüm bilgileri daha sonra yapılabilecek olan analizler ve ölçümler için saklayan bir bloktur. Bu blokların tümü veri alışverişlerini IETF tarafından belirlenmiş olan veri değişim biçimlerini ve protokollerini (RFC 4767 – IDXP, ‘‘Intrusion Detection eXchange Protocol’’ ve RFC 4765 – IDMEF, ‘‘Intrusion Detection MEssage Format’’) kullanarak gerçekleştirmektedirler [6].

IDS'ler daha önce karşılaşılmayan saldırıları algılayacak bir şekilde geliştirilmelidirler. Bir saldırı tespit edildikten sonra ise gerekli tedbirlerin alınması gerekir. Bu nedenle, tespit ve önleme sistemleri bir arada düşünülmelidir. Algılama ve tespit sistemi, önleme sisteminden bağımsız olarak geliştirilebileceği gibi beraberde geliştirilebilirler. Bu şekildeki çözümler Saldırı Tespit ve Önleme Sistemi (IDPS) olarak adlandırılmaktadır.

IDS'ler genel olarak iki ana grupta sınıflandırılabilir [7]. Birinci grup kullanıcı ya da sunucu bilgisayarlarına kurulan yazılım tabanlı sistemlerdir (host-based). İkinci grup ise ağ tabanlı (network-based) olarak tasarlanmıştır. Ağ tabanlı sistemler kendilerine ait özel donanımlar ya da kendilerine tahsis edilmiş ayrı bilgisayarlar üzerinde çalışırlar. Bir yazılım tabanlı IDS, ağ kartını, işletim sisteminin sistem çağrılarını ve yüklü olduğu bilgisayarda çalışan programların davranışlarını izler. Öte yandan ağ tabanlı bir IDS, basit bir şekilde ifade etmek gerekirse yerel ağa gelen ve giden veri trafiğini, her tür olayı ve bilgisayarlar arasındaki iletişimi takip ederek analiz eder. Kısaca, trafik hacmi, İnternet Protokolü (IP) adresleri, servis portları, protokol kullanımı vb. ağ ile ilgili tüm kriterler dikkate alınır [8]. Bu kapsamda, IDS saldırıları yetenekleriyle tanımlamaya çalışarak genel ağ güvenliğine önemli katkılarda bulunur. Bir kez ağda yeni bir saldırı türü belirleyen bir IDS, saldırının imzasını kendi veri tabanına kaydederek gelecekte karşılaşabileceği benzer veya aynı saldırılara karşı daha hazırlıklı hale gelebilir. Bununla birlikte, aynı anda farklı bir ağda çalışmakta olan başka bir IDS, böyle bir saldırı ile daha önce karşılaşmamış olabilir ve daha da kötüsü, karşılaştığı zaman tespit etmede yetersiz kalabilir. Bu amaçla bir çözüm olarak, IDS'ler arasında önemli görülen bulguların paylaşılabileceği düşünülmektedir. Böylece, bu yeteneğe sahip olan bir IDS, aynı hatanın başka IDS'ler tarafından yapılmasını önleyebilir. Sonuçta farklı üreticilere ait IDS'ler arasında veri paylaşımını sağlamak maksadıyla standart bir veri alışveriş biçimi kullanılmasının önemi ortaya çıkmaktadır.

IDS'ler üzerinde çalışılırken performansları yönünden karşılaştırma yapabilmek çok önemli bir yetenektir. Yanlış Alarm Oranı ve Algılama Oranı genellikle kullanılan iki temel performans ölçütüdür. Algılama Oranı, doğru algılanan saldırı sayısının (alarm üretilen), tüm saldırıların sayısına oranıdır. Yanlış Alarm Oranı ise, normal bir olayın saldırı olarak varsayıldığı durumların, normal olayların tamamının sayısına oranıdır. Sayılan bu iki durumda da IDS'in alarm verdiği durumlardaki

performansının ölçülmesi amaçlanmaktadır. Bazı durumlarda ise IDS'ler herhangi bir alarm üretmezler. Başka bir deyişle, gerçek bir saldırı olduğunda verilemeyen bir alarm tekrar kötü performans anlamına gelirken, normal ağ etkinlikleri sırasında IDS'in alarm üretmemesi de iyi performans anlamına gelmektedir. Bu dört farklı durum, temel olarak, performans oranları ile birlikte Şekil 1.2'de sunulduğu gibi hep birlikte IDS performans göstergeleri olarak ele alınmaktadır [1,9,10].

True Positive (TP):	Saldırı var – Alarm üretildi
False Positive (FP):	Saldırı yok – Alarm üretildi
True Negative (TN):	Saldırı yok – Alarm yok
False Negative (FN):	Saldırı var – Alarm yok
Tespit Oranı:	TP / Tüm saldırıların sayısı
Hassasiyet Derecesi:	(TP + TN) / Tüm olayların sayısı
Yanlış Alarm Oranı:	FP / Tüm normal olayların sayısı
Doğruluk:	TP / Tüm alarmlar

Şekil 1.2 : IDS Alarm Durumları ve Performans Ölçütleri

1.2 Tezin Amacı

Bu tez çalışmasında öncelikle bahsedilen bütün bu yaklaşımlar ve türevleri genel olarak incelenmektedir. Daha sonra, performanstan ödün vermeden en iyi sonuçları verebilen yaklaşımlara sahip bir hibrid anomali tespit sistemi tasarlanması amaçlanmıştır. Bu amaçla, farklı alanlarda da kullanılan zaman serileri arasında uyumsuz verilerin bulunmasını sağlayan hareketli ortalama alma yöntemleri ve bilgiye dayalı algılama tespit sistemleri bir çatı altında toplanmıştır. Nispeten basit matematiksel işlemlerle çalışan bilgiye dayalı bir algılama tespit sistemine sahip IDS'in, saldırıları ve anormallikleri tespit ederken daha az bilgisayar kaynağı kullanacağı öngörülebilir.

2. AĞ PAKETLERİNİN ANALİZ TEKNİKLERİ

2.1 Yaklaşımlar ve İlkeleri

Bugün, bilginin güvenli ve doğru bir şekilde saklanması ve aktarılmasını sağlamak için yüksek seviyede güvenlik önlemleri alınması çok önemlidir. Bununla birlikte, İnternet veya başka herhangi bir ağ üzerinden güvenli iletişim, her zaman kötü niyetli kullanıcıların tehdidi altındadır [11]. Bu nedenle IDS'ler bilgisayar ve ağ güvenliği konusunda gerekli bir unsur haline gelmiştir. Genellikle bir siber saldırgan, bir bilgi sisteminde izin verilmeyen bir eylemi gerçekleştirmeye çalışan, bu amaçla hazırlanmış bir program veya kişi olarak tanımlanır. Bu şekildeki eylemler, bilginin bütünlüğünü, gizliliğini ve erişilebilirliğini tehdit eden, bilgi güvenliği hususunda risk yaratan her türlü eylemlerin bütünüdür [12].

Şekil 2.1 : Bütünlük, Gizlilik, Erişilebilirlik.

Bu noktada, IDS'ler olası saldırıları yakalamak için birçok farklı yaklaşıma göre tasarlanmaktadırlar [4,5]. Bu yöntemler, imza tabanlı ve anomali tabanlı olmak üzere iki ana başlıkta sınıflandırılabilir. Bu çalışmada, ağırlık merkezi anomali tespiti ve onun üç alt ana grubu olan İstatistik Tabanlı, Bilgi Tabanlı ve Makine Öğrenme Tabanlı yaklaşımlardır [1].

2.2 Yakalanan Paketler İçin Ön İşlem Yöntemi

Ağ iletişiminin doğası gereği ağa bağlı bir işletim sisteminde alınan ve gönderilen birçok ağ paketi bulunmaktadır. Bu paketlerin tamamının bir IDS tarafından ele alınmasının, analiz için tüm verilerin doğrudan analiz bloğuna gönderilmesinin, yüksek işlem gücü ihtiyacına ve sistem kaynaklarının ciddi şekilde boşa harcanmasına neden olacağı açıktır. Yakalanan paketler, sensör bloğu tarafından analiz bloğuna gönderilmeden önce en temel kriterlere göre ön filtreden geçirilirler. Böylece, analiz edilmesi gerekli olmayan bölümler dışarıda bırakılmış olur. Bu noktadan sonra, IDS aldığı ağ paketlerini analiz edecektir.

Sensör bloğu filtreleme sürecini şu şekilde uygulamak uygun olacaktır. İlk olarak korunması hedeflenen sistemde analiz için kullanılması planlanan paketlerin hangileri olduğu belirlenir ve tamamının gelen ağ trafiği içinden seçilmesi hedeflenir. Ön filtreleme, analiz öncesinde sistem kaynaklarının verimli kullanılması için büyük önem taşımaktadır. Bu amaçla ilk önce ağ katmanındaki trafik içinden, gelen IP ve İnternet Kontrol Mesajı Protokolü (ICMP) paketlerinin seçiminin uygun olacağı değerlendirilmiştir. Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP) ve benzeri diğer paketler analiz sisteminde değerlendirilmemiştir. İletim katmanı düzeyinde ise, uygulama katmanının port numarasına bakılmaksızın, inceleme için Transmission Control Protocol (TCP) ve User Datagram Protocol (UDP) paketleri seçilmişlerdir.

Ağ üzerindeki her noktadan gelen tüm verilerin sürekli izlenmesi ve analizi, sistem kaynakları üzerinde ciddi bir yük yaratacağı yukarıda açıklanmıştı. Bu nedenle, mevcut CIDF yapısına ek olarak [6], risk değerlendirmesini gerçekleştirebilecek yeni bir blok yapısına sahip olunması ve buna göre de analiz bloğunun yönlendirilmesi uygun olacaktır.

İlk olarak, Risk Değerlendirme Bloğu muhtemel saldırı noktalarını ve yöntemlerini içermelidir. İkincisi, başarılı bir saldırıda ne kadar zararın oluşabileceği önceden tahmin edilerek sistemin kritik noktaları ortaya çıkarılmalıdır. Bundan sonra, riskleri azaltmak için gereken maliyet (sistem kaynağı) hesaplanmalı ve değerlendirmeye dâhil edilmelidir. Carl von Clausewitz tarafından tanıtılan Ağırlık Merkezi kavramı gibi, risk değerlendirme kabiliyeti, IDS'in önemli olan noktalara fazladan kaynak kullanmadan daha fazla dikkat etmesini sağlayabilir.

2.3 Analiz Yaklaşımları

2.3.1 İstatistik tabanlı analiz

İstatistik Tabanlı tespit sisteminde, IDS "normal" olarak kabul edilen ağ etkinliğini izleyerek istatistiksel bir model, normale ait olan bir desen oluşturur. Başka bir deyişle, ağ trafiğini gözlemleyerek her olay için olasılıklara dayalı bir davranış modeli oluşturur. Modele, desene uymayan, normal olarak belirlenen aralık dışında kalan herhangi bir ağ trafiği anomali olarak işaretlenir [16] çünkü olağan dışı olaylar güvenlik açısından şüphelidirler.

Uygulamada, istatistiksel hesaplamaların düzenli aralıklarla yapılmasına ihtiyaç vardır. Sürekli değişen ağ ortamında yanlış alarmlar üretilmesinin önüne geçilebilmesi ve gerçek saldırıların da gözden kaçırılmaması gerekmektedir. Daha uzun süre gözlem yapıldığında, daha başarılı bir tahmin yapmak da mümkün olmaktadır. Fakat gelişmiş istatistiksel uygulamalar taşınabilir bilgisayarların performansı ve bunların şarj edilmeden kullanım süreleri hakkında kaygılara neden olabilecektir.

Güvenliği sağlama noktasında, bu yöntemin tek başına yetersiz olduğu kabul edilmekle birlikte, aynı zamanda bir hibrid IDS'in de vazgeçilmez bir parçası [17] olduğu da bilinmektedir. Bununla birlikte, ne kadar da yararlı bir yöntem olsa da, kötü niyetli kişilerce varlığı tespit edildiğinde istenen yönde eğitilebilir. Bu önemli bir dezavantajdır, ancak bu yaklaşım her ne kadar tam olarak bir anomaliyi sıfır gün saldırısı olarak etiketliyemiyor olsa da belirli bir seviyede etkilidir.

2.3.1.1 Tek değişkenli analiz

Tek Değişkenli analiz, İstatistik Tabanlı yaklaşımın basit uygulamalarından biridir. Her olay için bir değişken tanımlanır ve normal bir dağılım ile modellenir. Bu yaklaşımın temel amacı, veri kümelerindeki desenleri bulmaktır [1].

2.3.1.2 Çok değişkenli analiz

Doğal olsun veya olmasın, çoğu olay çok değişkenli bir yapıya sahiptir. Bu yöntemde birbirine bağlı olaylar için birden fazla değişken tanımlanır ve aralarındaki korelasyon ölçülür [18]. Yapılacak olan ölçümlerde aynı şekilde birden fazla yöntem beraber kullanılabilir. Örneğin normal dağılımla birlikte Poisson dağılımları [19] beraber kullanılabilir. Çok değişkenli analizin birçok farklı türü vardır. Bu çalışmada, bazı özel çok değişkenli analiz yöntemleri seçilmiş ve Üçüncü Bölüm Önerilen Anomali Tespiti Tekniği altında tanımlanmışlardır.

2.3.1.3 Zaman serisi model analizi

Zaman serisi modelinde belirli bir zaman aralığında meydana gelen olayların frekansları, oluş sıklıkları değerlendirilir. Zaman serileri, değişkenlerin değerlerinin bir dönemden diğerine [20] sıralı olarak takip edildiği sıralı sayısal niceliklerdir. Zaman serileri, durağan ve durağan olmayan iki ana başlık altında incelenebilir. Bu amaçla, Poisson dağılımı, Chi-Square Goodness of Fit Test ve Least Squares Method yaygın olarak kullanılmaktadır.

2.3.2 Bilgi tabanlı analiz

Bilgi Tabanlı yaklaşım, IDS'lerde en yaygın olarak kullanılan tekniklerden biridir. Bu yaklaşımın uygulanmasında sınıflar, sınıflandırma kuralları, sistem değişkenleri ve tüm uygulama yordamları eğitim verilerinden belirlenir. Çalışma sırasında, sistem değişkenlerinin değerlerine göre, her bir olay için uygun olan yordamlar seçilerek uygulanmaktadır [21]. Bu kapsamda analiz bloğuna ulaşan veriler sınıflara ayrılarak, belirlemiş olan kurallara göre normal olup olmadıkları kontrol edilmektedir.

Kuralların oluşturulması sırasında kullanılacak sistem hakkında çok detaylı bilgiye ihtiyaç duyulmaktadır. Zor ve zaman alıcı olan bu safha, hazırlık aşamasının önemini ortaya koymaktadır. Fakat diğer yaklaşımlarla karşılaştırıldığında, en düşük miktarda sistem kaynağının bu yaklaşım tarafından kullanılması tercih sebebi olmaktadır.

Anomali tespitinde kullanılan kuralların hedef sistemin uzmanları tarafından hazırlandığından, bu yaklaşım aynı zamanda uzman sistem olarak da adlandırılmaktadır.

Model oluşturma aşamasının zorlu döneminden sonra inşa edilen IDS, dayanıklı bir yapıya kavuşmuş olur. Bununla birlikte, kurallardan oluşturulmuş olan anomali tespit modelinin daha sonra yapılacak olan her sistem güncellemesi ile birlikte güncellenmesi gerekecektir. Başlangıçta, esnek bir sistem vaat eden bu yaklaşım, tasarımcıların sürekli olarak güncellemesini gerektirir. Korunması amaçlanan sistemin davranışları daha önce modellendiğinden dolayı, yeni bir sıfır gün saldırısına karşı İstatistiksel Tabanlı yaklaşım kadar etkili olması beklenemez. Örneğin, işletim sistemindeki hatalı bir kod aracılığıyla başlayan bir saldırıyı yakalama şansı çok düşüktür. Aksine, İstatistiksel Tabanlı bir sistem, hatalı kod şüpheli olmasa bile elde ettiği sonuçlara bakarak gelen saldırıları tespit etme şansına sahip olacaktır.

Bilgi Tabanlı analiz kendi içinde birçok alt gruba ayrılmaktadır. Bu tez çalışmasında en önemli olanlar, nispeten basit olandan daha karmaşık olana göre sırasıyla aşağıda açıklanmıştır. Her bir grubun bir diğerine göre avantajları ve dezavantajları mevcuttur.

2.3.2.1 İmza tabanlı analiz

Bir ağdaki saldırıları tespit etmenin en temel yolu, bu saldırıları tanımlayan imzalar oluşturmak ve analiz safhasında kullanılması için saklamaktır. Olayların bu imzalarla karşılaştırılması sonucunda sisteme yönelik bir saldırı olup olmadığına karar verilmektedir [4]. İmza Tabanlı IDS'in bilinen virüslerin imzalarına bakarak arayan bir virüs tarayıcı gibi aynı şekilde analiz yapması anlamına gelir. Bu yaklaşımda bilinen saldırı türlerinin tespiti etkili şekilde yapılabilmektedir. Benzer şekilde daha sonra farklı yöntemlerle tespit edilen her yeni saldırının da imzası veri tabanına eklenerek üstünlük sağlanmış olacaktır. Bu, her IDS tasarımının sahip olması gereken önemli bir algılama sistemidir.

2.3.2.2 Uzman sistem (statik kurallar) analizi

Uzman Sistem tekniği saldırıların nasıl gerçekleştiklerini, sırasıyla hangi adımları izlediklerini temel alarak analizler yapmaktadır. Bir kısım saldırıların farklı hedefleri

olsa da, farklı imzaları olsa da, hedeflerine giderken aynı yolları kullanır ve aynı sistem yordamlarını çağırırlar. Saldırıların uyguladığı bu ortak faaliyetler bir kural olarak ifade edilmektedir. Böylece benzer saldırılar imzalarını değiştirmeye yönelik tedbirler geliştirmiş olsalar bile IDS tarafından tespit edilebileceklerdir. Bunun yanında saldırısını aynı yolları kullanarak gerçekleştirmeye çalışan yeni bir tür saldırı da sistem tarafından yakalanabilecektir. Esasında IDS yeni bir saldırıyı yazılmış olan kurallara göre tam olarak saldırı olarak etiketlemez.

Genellikle bu durumda uygun olan davranış olayın şüpheli olarak belirlenmesi ve rapor edilmesidir. Gerçekleşmekte olan olaylar beklenen sırada ise tamamının şüpheli olarak sınıflandırılması doğru olacaktır. Özetle saldırı kurallarına bakarak analiz yapan bir IDS, kuralların ihlal edilip edilmediğini kontrol eder [1]. Örneğin, başka bir kullanıcıya ait olan yazma korumalı bir dosyaya yazılmaya çalışılması veya değiştirilmesi, sistem dosyalarının değiştirilmesi, önceden belirlenmiş normalden fazla dosya kopyalama işlemleri uzman sistemi kurallarına arasında sayılabilir.

2.3.2.3 Durum geçiş analizi

Durum Geçişi, sistem süreçlerinin çalışması sırasında sistemle ilgili özelliklerin bir durumdan diğerine geçişini temsil eder. Bu geçişlerin belirli bir işleyiş sırasını izlemesi beklenir. Durum Geçiş Analizinde (STA) belirli bir etkinlik sırasında beklenen bu sıralı işlemlerin sırayla gerçekleştirilip gerçekleştirilmediği kontrol edilir. Örneğin, korumalı bir dosyayı değiştirmeden önce başarılı bir kimlik doğrulaması yapılmalıdır. Bir saldırının doğasında, amaçlanan işlemlerin gerçekleştirilmesi için hedef sistem üzerinde bir dizi durum değişikliği yapmak vardır.

Bu yaklaşım içinde başarılı bir saldırı öncesi mutlaka sistem üzerinde değiştirilmesi gereken durumlar tespit edilmektedir. Böylece saldırı eylemine odaklanmak yerine sonuçlara bakarak farklı eylemleri gerçekleştiren farklı saldırılar belirlenebilir. Sonuç odaklı yaklaşım sayesinde STA, sistemde bulunan kodlama hataları sonucu oluşan güvenlik açıklıklarını kullanarak gerçekleştirilen saldırıları daha teşebbüs safhasında tespit edebilmeyi vaat etmektedir [22].

2.3.2.4 Petri ağları

Klasik STA'da, olaylar sırayla birbirini izlemelidir ve STA bu sırayı takip ederek bir saldırı olup olmadığına karar vermektedir. Ancak, gerçek hayatta her zaman bir saldırı beklenen bir sırada eylemlerini uygulamak zorunda değildir. Bir saldırının uygulayacağı adımların sırası değişebilir veya bazı adımlar aynı anda gelişebilir. Zamana göre beklenen olay akışı tamamen değişerek bir noktadan itibaren çok farklı yeni adımlar gerçekleşebilir. Bu bakımdan bu gibi saldırılara karşı kural yazımı için Petri Ağlarının kullanılması oldukça yararlı olacaktır. Petri-net, 1962'de Carl Adam Petri tarafından tasarlanan, bir sistemin paralel ve dağıtılmış olaylarını modellemenin temel bir yoludur. Bir petri ağı, durumlardan ve durumlar arası geçişlerden oluşan çift kümeli bir grafik gösterim şeklidir temelde. Grafikte durumları ifade eden noktalar ile geçişleri ifade eden noktalar birbirlerine yönlü oklar ile bağlanmışlardır [13].

2.3.3 Makine öğrenme tabanlı

Yapay zekânın bir altkümesi olan makine öğrenimi, karmaşık yapıları verilerden tanımlamayı mümkün kılar. Temel olarak karar vermede istatistik bilimini ve bilgisayarların hesaplama gücünü kullanır. Ayrıca Makine öğrenimi uygulamaları karmaşık verileri sınıflandırmada oldukça başarılıdırlar. Bu kabiliyete ulaşılabilmesi için bir IDS'in saldırı tespit etme safhasından önce öğrenme aşamasını tamamlaması istenir. Bu aşamadan sonra sistem, sınıflandırmada kullanabileceği bir model oluşturur.

Makine öğrenmesi, istatistiksel tabanlı bir yaklaşım gibi sınıflandırma ve analiz uygulamakta olsa bile, geri beslemelerle sınıflandırma ve analiz modelini geliştirebilir. Bu yönü sayesinde sıfır gün saldırılarına karşı gayet kullanışlı ve istikrarlı bir yapı sunabilmektedir. Bununla beraber daha yüksek bir başarılı tespit etme oranına sahip olmasına rağmen, sistem kaynakları üzerinde ciddi bir yük oluşturması da kaçınılmazdır. Bu yaklaşımda öncekiler gibi kendi içinde alt gruplara ayrılmaktadır. Temel olarak makine öğrenme teknikleri arasında Bayes Ağları, Yapay Sinir Ağları, Bulanık Mantık Teknikleri, Genetik Algoritmalar ve Kümeleme ve Sınır Algılama [1,23] sayılabilir.

3. ÖNERİLEN ANOMALİ TESPİT TEKNİĞİ: BİLGİ TABANLI İLE ÇOK DEĞİŞKENLİ ZAMAN SERİSİ MODELİ

3.1 Gerekçe

IDS tasarımının en önemli parçası hiç kuşkusuz saldırıları tespit etmekten sorumlu olan analiz bloğu olduğu açıktır [6]. Bu blok içinde bir önceki bölümde listelenen yaklaşımlardan bir ya da birkaçının birlikte işleyeceği bir yapı kurulması amaçlanmıştır. Değerlendirilen her bir yaklaşımın birbirlerine göre ayrı ayrı üstün yönleri mevcuttur, fakat bunların hiçbirisi her yönüyle bir diğerinden daha üstün değildir [4,5]. Bu nedenle, karma, hibrid bir sistemin tasarlanarak uygulanmasının zorunlu olduğu değerlendirilmiştir. Bir önceki bölümde de ifade edildiği gibi güvenlik seviyesi için tespit başarısını arttırma gayretleri aynı zamanda sistem kaynak tüketimini de arttıracaktır.

Bu maksatla önerilen saldırı tespit sistemi içinde, tüketilen bilgisayar sistemi kaynakları ile kazanılan performans arasında uygun bir denge politikası izlenmiştir. Kaynak tüketimi dikkate alındığında sistemin bir parçası olarak İstatistik Tabanlı yaklaşımların kullanılmasının Makine Öğrenme tabanlı bir çözüme göre daha iyi bir başarım sunacağı, bu nedenle de gayretlerin bu yönde kullanılmasının uygun olacağı değerlendirilmiştir [1].

Bilgi Tabanlı yaklaşım, İstatistiksel Tabanlı yaklaşımı içeren bir hibrid IDS'nin tamamlayıcı parçası olarak seçilmiştir. Bilgi Tabanlı yaklaşım ile işletim sistemi yordamlarını takip etmek İstatistik Tabanlı yaklaşıma göre daha az kaynak ile daha kesin sonuçlar üretmektedir.

Bu amaçla öncelikli olarak IDS'in Bilgi Tabanlı yapısının oluşturulması amaçlanmıştır. Normal sistem çalışmasına ait olması gereken koşullar sırasıyla belirlemiş ve daha sonra İstatistiksel Tabanlı yaklaşım için, düşük kaynak tüketimi ile yüksek performans özelliklerine sahip olduğu düşünülen yöntemler sırasıyla açıklanmış ve uygulanmıştır.

3.2 Anormal Saldırıların Belirlenmesi

Bilinen bir saldırının belirlenmesi ve önlenmesi nispeten anormal özelliklere sahip bir saldırıdan çok daha kolaydır. Bu yüzden anormal olarak sayılabilecek etkinliklere sahip türde saldırıların her geçen gün hızla artması şaşırtıcı değildir. Bu alanda, benzersiz yeni teknikler barındıran, daha aldatıcı ve karmaşık şekilde karşımıza çıkan Hizmet Reddi (DOS) ve Dağıtılmış DOS (DDOS) saldırıları anomali sayılabilecek özellikler ortaya koymaktadırlar. DOS ve DDOS saldırıları, birçok kaynaktan gelen sürekli ve yoğun bir ağ trafiği ile genellikle sunucu kaynaklarını tüketmeyi, bilgisayar sistemlerini tepkisiz kılmayı ve ağ yönlendirici cihazlarını olabildiğince meşgul etmeyi amaçlamaktadırlar. Meşru kullanıcıların bilgisayar uygulamalarını kullanmalarını zor veya imkânsız hale getirmeleri ile de saldırılar hedeflerine ulaşmaktadır [14]. Yarattıkları etkilerin yanında uygulanmalarının basit oluşu saldırganlar tarafından daha çok tercih edilecekleri anlamına gelmektedir. Elbette bu durum ve yaşanan olaylar işletmeler ve kuruluşlar için günden güne artan bir güvenlik kaygısına da neden olmaktadır.

Tabii olarak, birçok yönden anomali özelliklere sahip DDOS saldırılarını açıklamak mümkündür. Günümüzün en tehlikeli saldırı türlerinden biri olan DDOS saldırılarını daha kolay anlamak için, üç ana başlık altında incelenmesi uygun olacaktır [15].

3.2.1 Yüksek yoğunluklu saldırılar

Her türlü ağ paketi seli dâhil olmak üzere UDP, ICMP ve diğer sahte başlık bilgisine sahip paketler bu sınıfta değerlendirilebilir. Hedef, kaynakları tükenene ve çevrimdışı hale gelene kadar kötü niyetli trafiğe maruz bırakılmaktadır.

3.2.2 Protokollerin kötüye kullanımı

Hedef sistemle ilgili bilgilerin toplanması ve uygun görülen protokollere birçok uygun şekilde hazırlanmış saldırı paketi gönderilerek istismar edilmesi durumudur. Geçersiz yaşam süresine sahip (TTL), aynı kaynak ve hedef portu işaret eden, adres ihlalleri içeren, geçersiz TCP bayrakları olan, port numarası içermeyen, zorla yönlendirme yapan ve çok kısa olan paketlerle yapılan saldırılar örnektir. İlave olarak senkronize olmayı engelleyen (SYN) paket selleri, sistemin işleyişini tamamen durduran ping çeşitleri (Ping of Death) ve Smurf DDoS bu tür saldırılara iyi birer örnektir.

3.2.3 Uygulama katmanı saldırıları

HTTP (Hypertext Transfer Protocol) üzerinde uygun olmayan şekilde Get/Post komutlarının kullanımı, Yüksek yoğunlukta DNS (Domain Name System) isteklerinin cevaplarına maruz kalınması, yüksek yoğunluklu SMTP (Simple Mail Transfer Protocol) üzerinde e-posta trafiği oluşması, düşük ve yavaş seyreden paket gönderimleri (Low-and-slow) bu katmanda karşılaşılan saldırılardır. Bu saldırıların hedefinde genellikle www hizmeti veren sunucu uygulamaları olabileceği gibi özellikle bir web uygulamasını da hedef olabilir. Web sitelerine ve IP haberleşme yapan programlara yapılan saldırılar bu kapsamda incelenmelidir.

3.3 Bilgi Tabanlı Kuralların Oluşturulması

Birçok DDOS saldırı çeşidi bulunmasına rağmen diğer tür saldırılarla karşılaştırıldıklarında uygulanmaları ve yapıları doğal olarak daha basittir. Bu sayede ileri derecede ağ veya sistem bilgisine ihtiyaç duyulmadan bir DDOS saldırısı planlanıp ve düzenlenebilir. Çoğu zaman yeni bir yöntem dahi keşfedilmesine gerek duyulmadan bilinen yöntemlerle etkili saldırılar düzenlenebilmektedir. Bu basitlik sadece saldırı yapan tarafa avantaj kazandırmamaktadır. Aynı zamanda sorumlu olduğu sistemi savunmaya çalışanlara, bu konuda yeni tedbirler geliştirmeye çalışanlara da avantaj kazandırmaktadır.

Her ne kadar yeterli derecede yoğun bir DDOS saldırısını tam olarak durdurmak ve tamamen önlemek için kesin bir çözüm bulunmasa da, bir DDOS saldırısının henüz başlangıç aşamasında tespit edilebilmesinin savunan tarafa önemli derecede üstünlük kazandıracağı açıktır. DDOS saldırılarının yapı gereği basit olması sayesinde onları tanımlamada kullanılacak olan kurallarında yapıları nispeten daha basit olacaktır.

DDOS saldırıları için Bilgi Tabanlı analiz yöntemi içinde kuralların oluşturulmasında öncelikli olarak normal IP adreslerinin belirlenmesi amaçlanmıştır. Anormallik sergileyen bir IP adresi genellikle diğerlerine göre daha fazla ağ trafiği içinde yer alacaktır. Elbette her zaman tek bir IP DDOS saldırısı içinde yer almaz. Kimi zamanda aynı paketleri gönderen, aynı uygulamaları aynı port numaralarından meşgul etmeye çalışan birçok farklı IP adresi de olabilir. Bu ve buna benzer durumlar için kurallar oluşturulmasına bu yöntem içinde ilk olarak karar verilmiştir. Mümkün olduğu kadar erken şekilde DDOS saldırılarının tespit edilebilmesi için

birçok kural belirlenmesine ihtiyaç duyulmuştur. Bu tez çalışmasında önerilen ilave kurallar aşağıya çıkarılmıştır.

Her haftanın ve ayın günü bir önceki gün ile kıyaslanır. Örneğin her pazar günü diğer pazar günleri ile ya da her ayın ilk günü diğer ayların ilk günleri ile karşılaştırılabilir. Önemli faaliyetlerin olduğu günler ya da yoğun ağ trafiğinin gerçekleşeceği bilinen günler, olağan günlerden yola çıkılarak elde edilen normal değerlerin bozulmaması için ayrı tutulur. Her zaman toplam canlı bağlantı sayısı ve yeni bağlantı istek sayısı, istek türleri ve içerdiği talepler göz önünde bulundurulur. Böylece beklenen trafik modeli oluşturularak kuralları belirlenmiş olur. Ayrıca karşılaştırma modeli içinde oluşacak olan sapmaların nedenlerini bulmak için analiz yapılır ve bu doğrultuda elde edilen sonuçlara göre kuralların güncellemesi gerçekleştirilir.

İnternet trafiği arasında arama motorlarının dizin oluşturmada kullandıkları programların da bulunduğu bilinmelidir. Bunların yarattığı trafiğin gerçek kullanıcı trafiğinden ayırt edilmesi daha gerçekçi analiz yapılabilmesi için gereklidir. Bu maksatla kurulan bağlantılar üzerinde ne tür biçimde veri akışı olduğu tespit edilir. Sadece HTML, XML ve benzeri sayfaların mı isteklerde yer aldığı yoksa diğer resim, stil şablonları gibi tüm nesnelerinde taleplerde yer alıp almadığı kontrol edilir. Bu kural aynı zamanda dizin oluşturma amacının dışında sistem kaynaklarını tüketmeyi hedefleyen programlarında tespit edilmesi için gereklidir.

Kimlik tanımlaması yapılmış kullanıcılar arasında bağlantı isteklerine olumlu cevap aldığı halde sürekli aynı adrese HTTP bağlantı isteği göndermeye devam edenler tespit edilir ve izleme listesine alınır. Benzer şekilde belirli bir IP adresinin birçok protokolü üzerinde sayısız portu ile haberleşmeye çalışan kullanıcılarda kural gereği bağlantıları kesilebilir. Yerel ağ içinde bulunan sunucuların kapalı olan protokol ve portlarına sürekli bağlantı isteği yapan kullanıcılar takip listesine alınır. İlave tedbir olarak ağ trafiğinin yoğunlaşmaya başladığı zamanlarda gerekirse tespit edilen bu kullanıcıların tüm bağlantıları da kesilebilir.

3.4 Bilgi Tabanlı Çok Değişkenli Teknikler

Bu tez çalışmasında Bilgi Tabanlı oluşturulmuş kuralların yanında anomali analizinde görev alacak olan çok değişkenli tekniklerden Hareketli Ortalamaların kullanılmasına karar verilmiştir. Hareketli ortalamaların tanımlanmasından önce

analiz bloğuna ulaşan paketlerin zamansal olarak gruplandırılmasına ihtiyaç vardır. İlk olarak her IP adresine göre paketler ayrılır. Bu paketler daha sonra alındıkları ya da gönderildikleri zaman dilimlerine göre kümelenirler [36]. Bu şekilde zamana ve adrese göre kümelenen paketlerin yoğunluk grafikleri oluşturulabilir. Grafiklerde seçilecek olan zaman dilimleri, ait oldukları IP adreslerine ve paketlerin özelliklerine göre seçilmelidir. Özellik olarak her bir grafiğin zaman dilimi 1 dakikadan 1 aya kadar geniş bir aralıkta değiştirilebilir. Yapılacak olan analizin sonuçlarını doğrudan doğruya etkileyeceği düşünüldüğünde oluşturulacak olan Bilgi Tabanlı kuralların ne kadar özenle belirlenmesi gerektiği açıktır. Özel bir kural belirlenmediği sürece zaman dilimleri 1 dakika ile 4 saat arasında değişecek şekilde belirlenmiştir.

Seçilen yöntemlerin önemli bir ortak bir özelliği kabaca zaman serileri olarak kümelenen verilerin ortalamalarını almalıdır. Fakat görünenin arkasında fazlası bulunmaktadır. Anomali tespitinde yenilikçi bir yaklaşım olarak sunulan bu yöntemler yıllardır başarılı bir şekilde finans dünyasında hali hazırda kullanılmaktadırlar [24]. Bu teknikler özünde ileri seviyede düzensizlik içeren veri kümelerinin anlam kazanmasında, belli bir seviyeye kadar düzenli ve anlamlı sonuçlar üretilmesinde rol almaktadırlar. Aynı şekilde bilgisayarların iletişim ortamında ki veri trafiği de doğrusal fonksiyonlarla ifade edilemeyen ileri seviyede düzensiz bir yapı sergilemektedir. Bu yönüyle aynı tekniklerin kullanılmasının yenilikçi bir yaklaşım olmasının yanında etkili bir analiz yöntemi olduğu da görülmüştür.

Ağ paketlerinin zaman şemaları hazırlandıktan sonra seçilen zaman aralıklarına göre analiz yapılarak anomali tespit edilecektir. Bu kapsamda sistem kaynaklarını ölçülü kullanan, nispeten basit hesaplama adımlarına sahip olan yöntemler sırasıyla aşağıda sunulmuştur.

3.4.1 Basit hareketli ortalama

İstatistik biliminde Basit Hareketli Ortalama (SMA) belirli bir t zaman dilimi içinde bulunan verilerin aritmetik toplamlarının zaman dilimi sayısına bölünmesi ile ilk değer hesaplanır. Takip eden diğer değerlerin hesaplanması için ise t zaman dilimi geçmişe doğru birer birer kaydırılarak hesaplama yenilenir. Hesaplamalarda grafiğe eklenen son veri ilk olarak ele alınır [25,27]. Örneğin 10 zaman dilimlik süre için son 10 verinin ortalaması alınır. Peşinden son veri dışarı atılarak 11. veri seriye eklenerek

yeniden ortalama alınır. Bu şekilde en başa kadar tüm ortalamalar alınır ve elde edilen ortalamalar grafiğe eklenir. Bu hali ile grafik hala analiz yapılabilecek durumda değildir. Ortalamaların gösterildiği çizgiye göre alt ve üst eşik değerleri de belirlenmelidir. Bu eşik değerlerinin ne kadar uzakta veya yakında olacağına Bilgi Tabanlı olarak belirlenen kurallara göre karar verilir. Bu teknik paket yoğunluğunun istikrarlı olduğu, herhangi bir eğilim veya mevsimsel değişim göstermediği durumlarda başarılı bir şekilde kullanılabilir. Dağınık duran veri setlerinin anlaşılır düz bir veri seti haline getirir [25,27]. SMA'nın hesaplama formülü aşağıda, örnek hesaplama ve analiz örnekleri Ek-A.1 ve A.2'de sunulmuştur.

$$SMA_n = \frac{\sum_{i=1}^{n} P_i}{n} \tag{3.1}$$

P_i: i periyodu için paket sayısı

n: hareketli ortalama için periyod sayısı

3.4.2 Üstel hareketli ortalama

Basit Hareketli Ortalama her periyottaki tüm veri setlerine aynı önemi gösterir. Ancak veri kümelerine en son eklenen veriler eskilerinden daha önemli ise kullanışlı bir yöntem değildir. Bu gibi durumlar için geliştirmiş olan Üstel Hareketli Ortalama (EMA), paket sayılarındaki artışlara ve azalışlara karşı daha duyarlıdır [25,27]. Böylece, EMA dönemsel ve mevsimsel dalgalanmalara karşı SMA'ya göre daha hızlı tepki göstererek çok daha sağlıklı bir analiz yapılmasına imkân verir.

EMA formülü aşağıda verilmiştir ve örnekleri Ek-A.3, A.4'te sunulmuştur. Denklem içinde bir önceki değere göre hesaplama yapıldığı için başlangıçta Basit Hareketli Ortalama kullanılabilir ya da doğrudan serinin ilk değeri önceki EMA olarak seçilebilir. İkinci olarak bir düzeltme katsayısı kullanılır. Bu katsayının alacağı değere göre analizin üreteceği değerler değişecektir. Katsayı 1 iken her türlü durum normal kabul edilir. Sıfıra yaklaştıkça da her türlü durum anomali olarak işaretlenir. Düzeltme katsayısının oluşturulmasında kullanılan periyot (n) uzunluğu arttırıldıkça anomali tespit hassasiyeti de artacaktır.

$$EMA_n = \big((P - Previous\ EMA) * \propto\big) + Previous\ EMA \quad (3.2)$$

P: bulunulan periyodun paket sayısı

$\propto$: düzeltme katsayısı $= \frac{2}{1+\mathrm{n}}$ [28]

n: hareketli ortalama için periyod sayısı

3.4.3 Ağırlıklı hareketli ortalama

Ağırlıklı Hareketli Ortalama (WMA) her bir veri grubunun bir ağırlık faktörü ile çarpılması ile EMA gibi en son verilere önceki verilerden daha fazla önem vermektedir. EMA gibi benzersiz hesaplamalar yapabileceği için, WMA verileri SMA'dan daha yakından takip edebilmektedir [26]. WMA hesaplama formülü aşağıda ve örnekleri Ek-A.5, A.6'da sunulmuştur.

$$WMA_n = \frac{\sum_{i=1}^{n}\big(P_i * (n+1-i)\big)}{\left(\frac{(n+1)*n}{2}\right)} \quad (3.3)$$

P_i: i periyodu için paket sayısı

n: hareketli ortalama için periyod sayısı

Ağırlık olarak rasyonel sayılarda kullanılabilmesine rağmen örneklerde konunun daha kolay anlaşılabilmesi için ağırlık faktörleri en son 1 olacak şekilde tam sayı olarak belirlenmiştir. Örneğin 20 periyot için ağırlıklar 20'den 1'e kadar birer birer azalarak devam etmektedir.

3.4.4 Hull hareketli ortalama

Alan Hull tarafından geliştirilen Hull Hareketli Ortalama (HMA), aslında bir seri grup WMA olan ve çok daha hızlı bir şekilde normal akışın normal sınırlar içindeki değişimlerini takip edebilen bir hareketli ortalama çeşididir [29,30]. HMA'da amaç, SMA, EMA ve WMA'da oluşan gecikmelerin olabildiğince önüne geçebilmektir.

HMA hesaplaması belirlenen (n) periyot sayısı için 3 farklı WMA hesaplanarak uygulanır. Yukarda anlatıldığı şekilde $WMA_{(n)}$ değerleri hesaplanır. Daha sonra, bu hesaplanan değerler ile $2*WMA_{(n/2)}$ değerleri arasındaki farklar alınarak yeni bir veri dizisi (d) oluşturulur. Son aşamada, yeni d veri dizisinin $WMA_{(sqrt(n))}$ değerleri bulunur. HMA formülü aşağıda sunulmuştur. Analizi ile birlikte örnekler Ek-A.7, A.8'de görülebilir. Örneğin n periyot 10 seçildi ise n/2 için 5 sayısı, karekök n için ise 3 sayısının kullanılması uygun olacaktır.

$$HMA_n = WMA_{(\sqrt{n})}\left(\left(2 * WMA_{(\frac{n}{2})}\right) - \left(WMA_{(n)}\right)\right) \quad (3.4)$$

n: hareketli ortalama için periyod sayısı

3.4.5 Değişim oranı

Bu noktaya kadar ardı sıra gelen paket yoğunlukları arasındaki ilişkileri belirlemek ve var olabilecek olan anomali durumlarının tanımlanması için çeşitli yöntemlerin nasıl kullanılması gerektiği örnekler ile açıklanmıştır. Tek başına bir analiz yöntemi olarak kullanılamayacak olsa da, anomali tespitinde yararlı olacağı ve kullanımının uygun olacağı değerlendirilen Değişim Oranı (ROC) yaklaşımı ile her periyottaki paket sayılarının bir önceki periyottaki sayılara göre olan değişim oranlarının hareketli ortalamaları ile belirlenecek olan eşik değerlerine göre anomalinin var olup olmadığı analiz edilebilir. Kullanılacak olan hareketli ortalama çeşidi önceden belirlenen kurallara göre seçilebilir. Bu teknikle, hareketli ortalamalar fark etmeden önce sistemde oluşacak olan ani değişimler çok yüksek bir hızla tespit edilebilir. Örnek uygulama Ek-A.9'da sunulmuştur.

3.5 Tekniklerin Birlikte Kullanılması

Anomali analizinde kullanılmaya uygun olarak değerlendirilen birçok uygulama yöntemi örneklerle açıklanmıştır. İlgili yöntemler incelenirken sistem üzerindeki hesaplama yükünün ölçülmesi ve yöntemlerin paket yakalama anında ve sonrasında başarıyla kullanılabilecek olması, her tekniğin farklı değişkenlerle farklı ihtiyaçları karşılayabilecek olması önemli birer avantajdır. Bu çok değişkenli teknikler bütünü anomalilerin saptanmasında hızlı ve ölçeklenebilir bir yapı sunmaktadır.

Sistemde tespit edilen anomalilere ilave olarak, yapılan değerlendirmeler içinde mutlaka gürültüye bağlı yanlış algılama, sahte uyarılarda oluşacaktır. Bu nedenle, hiçbir tekniğin tek başına güvenilir olamayacağı açıktır. Konu bu kapsamda değerlendirildiğinde önemli bir gereklilik ortaya çıkmaktadır. Gürültü oranı nasıl azaltılabilecektir? Bu sorunu çözmek için son olarak sunulan RoC ile diğer tekniklerin desteklenmesi uygun olacaktır. Buna ek olarak, seçilecek iki farklı yöntemin birlikte kullanılarak da analiz yapılması mümkündür.

Teknikleri bir arada kullanma bağlamında, en önemli konu, her tekniğin gerektirdiği değişkenlerin doğru bir biçimde belirlenmesi olacaktır. Değişkenlerin belirlenmesinde, uzman yardımıyla oluşturulacak olan kurallar ön plana çıkmaktadır. Burada Bilgi Tabanlı yaklaşımın önemi büyüktür. Farklı olaylar için farklı yöntemler, farklı düzeltme ve ağırlık katsayılarıyla çok farklı modeller oluşturulabilir.

3.6 Üstün ve Eksik Kalan Yönler

Anomali tespitinde kullanılması önerilen, yenilikçi bir yaklaşımla ortaya konan analiz metotlarından her birinin bir diğerine göre üstün ve eksik yönleri bulunmaktadır. Elde edilen sonuçlara göre, tekniklerin birlikte kullanılması durumunda mevcut eksik yönlerin ihmal edilebilir derecede azaldığı değerlendirilmiştir. Genel olarak veri analizinde tek değişken yerine çoklu değişkenlere sahip modeller kullanılmaktadır. Sunulan tüm yöntemlerde aynı yapıya sahiptir. Çok değişkenli teknikler, farklı veri kümeleri arasındaki ilişkileri istatistiksel olarak ortaya çıkarabilir ve ilerisini öngörebilirler. Bu tez çalışmasında DDOS saldırılarının anomali analizi ile tespiti için çok değişkenli yaklaşımlar incelenerek kullanılmıştır.

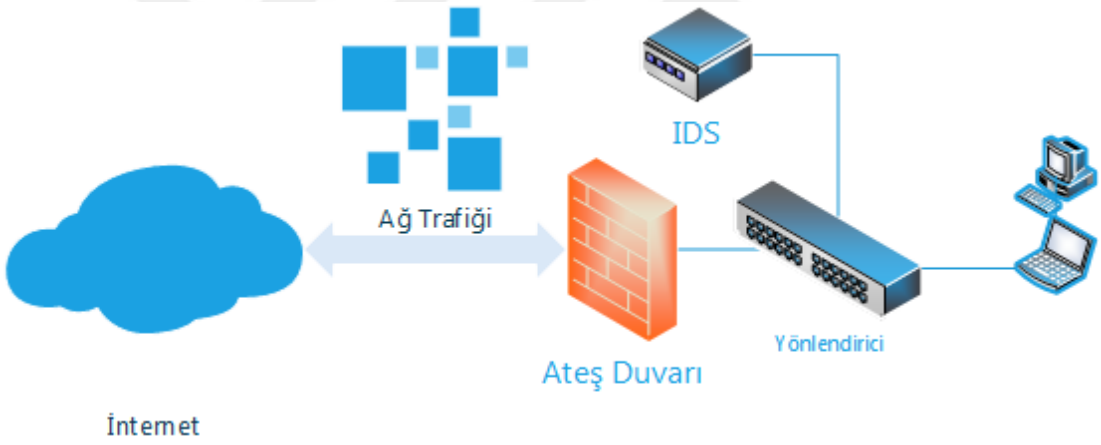
Çok değişkenli teknikler, IDS'lerin veri kümeleri arasındaki ilişkileri nicelleştirerek incelemelerine olanak tanır. Kolay uygulanmaları ve herhangi bir sistemde zahmetsizce çalıştırılmaları üstün olan yönleri arasındadır. Seçilen yöntemler ile bağımsız ve bağımlı değişkenler arasındaki ilişkilerin hangi şartlar altında oluştuğu belirlenebilir.

Bununla birlikte, bazen çok değişkenli teknikler, daha az tanınan ve çok karmaşık olan veri setlerini analiz etmek için daha yüksek istatistik hesaplamalarına ihtiyaç duyarlar. Bu durumda yüksek istatistiksel prosedürlerin uygulanmasına gerek duyulacaktır ancak maliyet etkin bir çözüm olmaktan da uzaklaşılacaktır. Bu tekniğin çalışmaya başlaması için uzun bir eğitim zamanına ihtiyacı olmadığı halde yeterli veri örneği ile beslenmediği zaman sağlıklı sonuçlar veremeyeceği bilinmelidir. Ağ trafiğinin izlemeye değmeyecek ölçüde sığ olduğu durumlarda elde edilecek olan sonuçlar gerçek durumu yansıtmayacak ve aynı zamanda sık sık yanlış alarmlara da neden olacaktır.

4. ANOMALİ ANALİZ MODÜLÜNÜN UYGULANMASI

4.1 Uygulama Mimarisi

Bir saldırı tespit sistemi her zaman sensörler ve analiz bloklarından oluşan çok çekirdekli bir yapıya sahiptir. Sensörler, ağ trafiği içindeki gelen ve giden verileri toplar ve uygun gördüklerini iletmek üzere paketler hazırlarlar. Yakalanan veriler başlangıçta analiz yapılmak için uygun durumda değildirler ve ön işlemci tarafından analiz edilmeye hazır hale getirilmeleri gerekir. Bunun için IDS mimarisi tasarlanırken uygun bir seçim mekanizması bölüm 2.2'de ifade edildiği gibi kurulmalıdır. Bu şekilde analiz bloğu gelen ve giden tüm veri akışı ile meşgul edilmemiş olur. Aşağıdaki şekilde örnek olarak ağ trafiğinin akışı sunulmuştur.



Şekil 4.1 : Ağ Trafiğinin Genel Akışı

Sensör bloğu, Şekil 1.1'de görülebileceği gibi yakalanan verinin zaman, IP numarası, protokol türü ve port numarasını veri tabanına ve analiz bloğuna iletir. IDS analiz bloğu, anlık ve kayıt edilmiş geçmiş veriler ile çalışabilecek şekilde tasarlanmıştır. Seçilen analiz yöntemlerinin farklı çalışma şekillerine uyumu ise bir başka üstün yön olarak değerlendirilmektedir.

Analiz bloğuna ulaşan filtrelenmiş veriler öncelikle IP numaralarına göre, peşinden protokol türlerine göre gruplandırılır. Zamansal olarak yapılan gruplama süreci analiz sürecinin temelini oluşturmaktadır. Zaman grupları, bir IP ile ilgili tüm paketlerin analizde seçilen zaman aralıklarına göre kümelenmeleri anlamına gelir.

Örneğin, 8.8.8.8 IP adresi tüm veri içinden seçilerek belirlenen her bir zaman dilimindeki mevcut sayısı ölçülür. Aşağıdaki çizelge 1 saatlik gruplamayı tasvir etmektedir.

Çizelge 4.1 : 1 Saatlik Gruplandırma

Day16.10.17-8.8.8.8.TCP.UDP.1h.table			
time	# of packets	Time	# of packets
00:00	0	12:00	3
01:00	0	13:00	6
02:00	0	14:00	0
03:00	7	15:00	0
04:00	7	16:00	91
05:00	27	17:00	0
06:00	17	18:00	0
07:00	3	19:00	0
08:00	0	20:00	0
09:00	13	21:00	0
10:00	4	22:00	0
11:00	0	23:00	0

Analiz tasarımının sağladığı esneklik sayesinde belirlenen zaman aralıkları kolayca ihtiyaca göre değiştirilebilmektedir. İstenen herhangi bir zaman dilim için yeni tablolar oluşturabilme özelliğine sahiptir. Aşağıdaki çizelge 4 saatlik gruplamayı tasvir etmektedir.

Çizelge 4.2 : 4 Saatlik Gruplandırma

Day16.10.17-8.8.8.8.TCP.UDP.4h.table			
Time	# of packets	time	# of packets
00:00	7	12:00	9
04:00	54	16:00	91
08:00	17	20:00	0

Benzer şekilde, bir saniyelik zaman aralığından aylık zaman aralığına uzanan farklı tablolar oluşturulabilir. Bu yapı sayesinde çok özel durumlardan genel görünüme kadar tüm gereksinimleri karşılamak üzere analiz yapılması mümkündür. Bilgi Tabanlı sistem tarafından ise hangi paket gruplarının hangi değişkenlerle hangi zaman aralığında analiz edileceğine karar verilir.

Hangi durumlarda hangi analiz metodunun kullanılacağına Bilgi Tabanlı yaklaşım ile karar verildiği ve kurallar oluşturulduğu daha önce ifade edilmişti. SMA ve EMA yöntemleri veri akışında anlık artış ve azalışların sık sık olmadığı veri grupları için kullanılmasına karar verilmiştir. Analiz edilecek veri grubu nispeten daha büyük ve geniş bir zaman dilimini kapsıyorsa, EMA'nın seçilmesine karar verilmiştir.

Kısa vadeli ve seyrek bir veri grubu varsa, SMA yöntemi kullanılacaktır. Her iki yöntemin yanında da, RoC yöntemi, momentumu, paket sayısının azalma oranını ve artışını belirlemek için seçilmiştir. Böylece, sistemin algılayacağı limit değerler aşılmasa bile, ani artışlar anormallik olarak işaretlenebilir.

Gelecekte ağda olması beklenen yoğunluğu hesaplamak ve hata oranını en aza indirgemek için, nispeten dağınık paket gruplarının analizinde daha karmaşık bir yapıya sahip olan EMA, WMA ve HMA kullanılacaktır. Saatlik, günlük veya haftalık olarak gerçekleşen düzenli – düzensiz değişimlerin, mevsimsel etkilerin en iyi şekilde modellenebilmesi ve oluşabilecek olan anomalilerin tespit edilebilmesi için kullanılmalarına karar verilmiştir. Bu yöntemlerde kullanılacak değişkenlerin seçimi yukarıda belirtildiği gibidir. Buna ek olarak, veri paket sayılarında ki ani değişiklikleri takip etmek için yine RoC yöntemi kullanılacaktır.

Son bölümde de açıklandığı gibi sonraki çalışmalarda değişkenlerin seçimi yapay zeka uygulamalarının yeteneklerine bırakılabilir. Böylece, daha yüksek verime sahip bir anomali tespiti, tamamen eğitim ihtiyacından bağımsız ve sistem hakkında önceden bilgi sahibi edinilmeden icra edilebilir.

4.2 Programlama Dili Seçimi

IDS analiz bloğu uygulamasında dikkate alınması gereken en önemli konu, sistem kaynaklarının ne kadarının analiz için kullanılacağıdır. Sistem kaynakları ne kadar az kullanılırsa, paket yakalamada kayıplar en aza indirilebilir ve önemli bir gecikme yaşanmadan eş zamanlı analiz yapılabilir. Bunu başarmak için akıllı algoritmaların yanında iyi düşünülmüş bir mimarinin de olması gerektiği açıktır.

Toplanan verilerin kurallara göre filtrelenmesi, kümelerin ve modellerin oluşturulması, analizlerin yapılması, veri kütük kaydının tutulması ve alarmların oluşturulması konuları en iyi başarımın sunulabilmesi için ayrı ayrı dikkatlice planlanmalıdır. Bunların gerçekleştirilebilmesi için genel özelliklere sahip güçlü bir programlama diline ihtiyaç vardır. Ayrıca programlanan bloklar daha sonra diğer alanlarda da bir seviyeye (yeniden kullanım) kadar kullanılabilir [31,32]. Aynı şekilde tasarlanan yapı sayesinde veri madenciliği yöntemleri gibi farklı alanlarda kullanılan yöntemlerde bu alana ithal edilebilir.

Linux işletim sistemi ortamında analiz bloğunun uygulanması için C++ programlama dili seçilmiştir. Ürettiği çıktıların hemen hemen her işletim sistemi altında kullanılabilmesini [34] sağlayan GNU [33] Derleyici programı (g++) C++ derleyicisi olarak seçilmiştir. Ayrıca, C++ dilinin seçilmesinde bir diğer neden, paket yakalama sisteminin yazıldığı dildir. Paket yakalamada kullanılan PCAP [35] kütüphanesi paket yakalama ve analiz bloğunun uyumlu bir şekilde çalışmasında önemli bir yere sahiptir. Bütün bunların yanında C++, genel amaçlı bir programlama dili olup, yerleşik işlevler sağlayan çok zengin bir kütüphane desteğine sahiptir. C++, programcıların düşük seviyeli programlamalarına olanak sağlamaktadır. Doğrudan Assembly Programlama Dili ile yazılmış program parçaları C++ kodları arasına eklenebilir.

4.3 Bütünleşik Geliştirme Ortamı (IDE)

Analiz modülünün geliştirilmesinde yukarıda belirtildiği gibi Linux İşletim Sistemi ortamında g++ derleyici (GNU C++ derleyicisi) kullanılmıştır. Analiz bloğu verileri bir metin dosyası ile zaman sırasına göre geldiğinden, Packet Capture (PCAP) kitaplıkları derlemeye dâhil değildir. My Structured Query Language (MySQL) veri tabanı kullanılırsa, dosya yapısına göre bağımsız bir çözüm olacağı için elde edilen sonuçlar daha sonra başka ortamlara kolayca iletilebilir. MySQL'in genel performansa olan etkisini sınırlamak için yalnızca oluşturulmuş modeller, modellerde kullanılan değişkenler ve alarmlar veri tabanına kaydedilmelidir. Derlemeye, sınırlı ve sadece gerekli olan matematik fonksiyonlarını içeren, yaygın olarak kullanılan bir C++ matematik kütüphanesi de eklenmiştir.

Gelecekteki çalışmaların Yapay Sinir Ağı (ANN) ile devam edeceği düşünüldüğünde derlemeye bir ANN kütüphanesi ve uygulama prosedürleri eklenmiştir. Bunun amacı, uzman yardımıyla tanımlanan değişkenlerin yapay zekâ tarafından bulunabileceği ve kullanılabileceğini göstermektir. Son olarak giriş-çıkış ve dosya okuma-yazma işlevlerini yerine getirmekten sorumlu olan standart C++ kütüphaneleri derlemeye dâhil edilmiştir. Performans ölçümü ve hata ayıklama için ayrıca bir kütüphane dosyasına başvurulmamıştır.

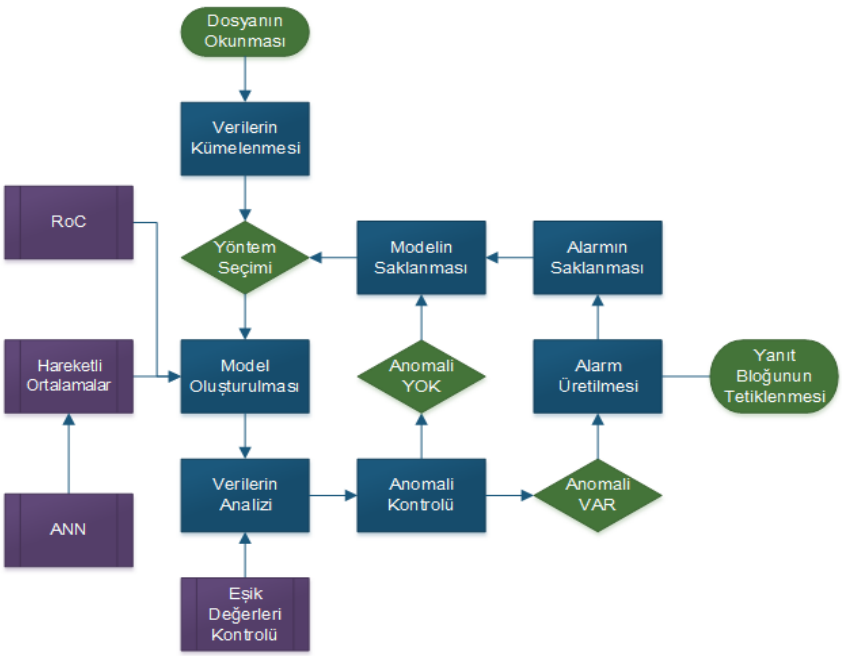
4.4 Yazılım Tasarımı

Analiz bloğunun programlanması sırasında, Linux işletim sistemi ortamında g++ derleyicisinin kullanıldığı yukarıda belirtilmişti. Bu kapsamda, program ilk önce ham metin dosyasını okumaya başlayacaktır. Metin dosyasında ki veriler aşağıdaki çizelgede sunulmuştur.

Çizelge 4.3 : Analize Sunulan Dosya İçeriği

time	IP	Protocol	Port
34064	x.x.x.x	TCP	52
34064	x.x.x.x	TCP	52
34064	x.x.x.x	TCP	60
34064	x.x.x.x	TCP	52
34064	x.x.x.x	TCP	52
34065	x.x.x.x	TCP	569
34065	x.x.x.x	TCP	52

Okunan veriler kümeleme için işlenir [36]. Kümeleme işleminde kullanılacak filtrelerde değişkenler, anomalinin nerede arandığına göre belirlenecektir. Örneğin, amaç bir IP numarası, belirli bir bağlantı noktası numarası veya belirli bir zaman aralığı olabilir. Daha sonra kullanılacak olan analiz metodu seçilecektir. Bölüm 4.1'de açıklandığı gibi, analiz için iki farklı yöntem bir yardımcı bir yöntem (RoC) ile birlikte kullanılacaktır. Anomalilerin saptanmasında kullanılacak olan modeller bu safhada oluşturulmuş olacaktır. Süreç aşağıda sunulan akışı takip etmektedir.



Şekil 4.2 : Yazılım İş Akış Şeması

Analiz bloğunun en önemli parçası olan algılama kısmı, belirlenen eşik değerlerine uygun olarak çalıştırılarak anormalliklerin tespit edilmesine çalışılır. Aynı zamanda, tespit edilen vakaların bir gürültü nedeniyle olup olamayacağı konusunda bir karara varılmaya çalışılır. Gerçekçi sonuçlar üretilmeye çalışılırken, daima yanlış alarmlara neden olabilecek olan gürültünün sistemde mevcut olduğu bilinmelidir. Bu nedenle, farklı yöntemleri kullanarak gelen verilerin çeşitli kontrol aşamalarından geçirilmesi üzerinde durulmuştur.

Tespit sistemi, kontrol sonucunda herhangi bir anormallik bulunmadığından emin olursa, analizde kullanılan model veri tabanına kaydedilmek üzere kayıttan sorumlu bloğa iletilir. Bununla birlikte, bir anormallik bulunması halinde ise hemen bir alarm üretilir ve yöneticiye bir uyarı gönderilir. Aynı zamanda, gerekli güvenlik önlemlerinin alınması için yanıt bloğu da tetiklenir. Son olarak, oluşturulan alarm bilgileri ve algılama için kullanılan model yine kayıt için veri tabanına gönderilir. Böylece, bir tespit döngüsü tamamlanmış olur.

Dikkate alınması gereken bir başka önemli husus, analizde kullanılan eşik değerlerinin seçimidir. Bu değerler, gürültünün hangi seviyeden itibaren gerçek alarm olarak değerlendirileceğini ve gerçek anomalilerden ne kadarının normal olarak görüneceğini belirler. Eşik değerlerinin belirlenmesi safhasında sayısal sonuçlar üretecek şekilde bir risk analizi yönteminin belirlenmesinin uygun olacağı değerlendirilmiştir. Risk analizinin nasıl yapılacağı detaylı olarak anlatılmayacaktır fakat korunan verilerin değeri ve yok oldukları zaman oluşacak olan zarar, bir risk analizi için temel girdi olarak kullanılmalıdır. Risklerin ne kadarının kabul edileceğini ve ne kadarının hafifletilebileceğini de belirlemek gerekir. Burada önemli olan soru "Riskleri nasıl azaltacağım?" olmalıdır. Bilginin güvence altına alınmasının yalnızca bilgisayarlarda kurulu olan güvenlik sistemleri ile sağlanamayacağı, ancak fiziki ve personel güvenliği konularının da genel bilgi sistemi güvenliği için hayati önem taşıdığı bilinmelidir.

4.5 Test Ortamı ve Sonuçlar

Test ortamı olarak standart dağıtım paketleri ile kurulmuş olan Debian 9.2 "Stretch" Linux işletim sistemi kullanılmıştır. Donanım olarak, x86-64 mimarisi olan bir masaüstü bilgisayar seçilmiştir. İşletim sistemine ek olarak, MySQL veri tabanı ve Yapay Sinir Ağı uygulaması için çok kullanışlı bir kütüphane olan Hızlı Yapay Sinir

Ağı (FANN) kütüphanesi de kurulmuştur. Önceden yakalanan paketlerin bilgilerini ihtiva eden düz metin dosyaları, bölüm 4.4 Yazılım Tasarımı bölümünde açıklandığı gibi girdi olarak kullanılmıştır. Analiz ve algılama sisteminin aldığı verileri kümelemesi ve bunlara bakarak modeller oluşturması beklenir. Daha sonra, normal modelin oluşturulması sırasında, eşik değerlerini aşan verilerin anormal olarak işaretlenmesi ve alarm üretim durumu kontrol edilir.

Test sonuçları incelendiğinde normal durumu ifade eden modellerin beklendiği gibi doğru bir şekilde tespit edildiği görülmüştür. Ardından gerçekleştirilen testlerin çıktılarında normal modellerle uyuşmayan yapıların işaretlendiği takip edilmiştir. Bu aşamada, hemen hemen her anomalinin doğru tespit edilmesinin yanı sıra, bazı durumlarda sistemde mevcut gürültüye bağlı olarak gelişen sahte anomalilerden ötürü yanlış alarm üretildiği gözlemlenmiştir. Sistem tasarlandığı gibi birden fazla tespit yöntemini kullanmıştır. Ayrıca, ANN tarafından üretilen değişkenlerin eşik düzeylerini belirlemede başarıyla kullanılmıştır.

5. SONUÇLAR VE GELECEKTEKİ ÇALIŞMALAR İÇİN ÖNERİLER

Bu tez çalışmasında ilk olarak bilgisayar ağlarının hızla nasıl büyüdükleri, kapasitelerinin ve yeteneklerin artması ile günlük hayatı nasıl kolaylaştırıldığı anlatılmıştır. Neredeyse sunulan her hizmet, internet ortamının yardımıyla daha verimli hale gelmiştir. Elbette bu gerçek, yasadışı yollarla kazanç elde etmek isteyenlerin, başkalarına zarar vermek isteyenlerin, devletlere ve kurumlarına saldırmak isteyenlerin de dikkatini çekmiştir. Bilgisayar ağlarına zarar vermek üzere tasarlanan ve kullanılan programlar vasıtasıyla gerçekleştirilen saldırıların boyutu, yarattıkları etki her geçen yıl artmaktadır. Siber uzayda meydana gelen bu saldırılardan korunmak ve mümkün olduğu zamanlarda durdurabilmek için gelişimleri halen devam eden IDS'ler kullanılmaktadır.

IDS endüstrisi hızla büyüyen yapısıyla güvenlik sistemlerinin vazgeçilmez ana unsurları arasında yer almaktadırlar. Bununla birlikte, üretilen çoğu IDS yaygın olarak kabul gören algılama yöntemleri içermektedir. Bu tezde tarif edilen yeni yaklaşımlar, ileride yapılacak olan çalışmalara ve son kullanıcı ürünleri için ışık tutacaktır. Belirlenen yöntemler ile artık, normal ve anormal sayılan ağ trafiğinin pratik ve hızlı bir şekilde modellenmesi mümkündür.

IDS ile ilgili yapılan birçok eleştiri genellikle iki konu üzerinde yoğunlaşmaktadır, performansları ve fiyatları. Bir IDS'in fiyatını belirleyen önemli bir bileşen, birim zamanda ne kadar ağ trafiğinin yakalanabileceğidir. Bir analiz yöntemi ne kadar iyi olursa olsun, ağ trafiği en iyi şekilde izlenmedikçe bilgi güvenliğinin kesin olarak sağlandığından emin olunamaz. Bundan sonra analiz sisteminin performansı hakkında değerlendirme yapmak yerinde olacaktır. IDS performansı doğru algılamanın ne kadar çabuk ve doğru bir şekilde yapıldığına göre belirlenmelidir. Bu noktada, savunulan yeni yöntemlerin IDS çalışmalarına önemli bir katkısının olacağı tahmin edilmektedir. Günümüzde ve büyük olasılıkla yakın gelecekte de siber saldırılar için kapsamlı ve kusursuz bir çözüm bulunamayacağı unutulmamalıdır.

KAYNAKLAR

[1] **P. Garcı´a-Teodoro, J. Dı´az-Verdejo, G. Macia´-Ferna´ndez, E. Va´zquez** (2008) Anomaly-based network intrusion detection: Techniques, systems and challenges.

[2] **F.Li, N.L.Clarke and M.Papadaki** (2008) Intrusion Detection System for Mobile Devices: Preliminary Investigation.

[3] **K. Scarfone, P. Mell** (2007) Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS) (2007), National Institute of Standards and Technology (NIST).

[4] **Priya U. Kadam, Prof.Manjusha Deshmukh** (2014) Various Approaches for Intrusion Detection System: An Overview, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 11.

[5] **Peyman Kabiri and Ali A. Ghorbani** (2005) Research on Intrusion Detection and Response: A Survey, International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005 (http://isrc.nchu.edu.tw/ijns/).

[6] **The Internet Engineering Task Force (IETF®)** (1998) The Common Intrusion Detection Framework - Data Formats (https://tools.ietf.org/html/draft-staniford-cidf-data-formats-00).

[7] **Url-1** <*https://www.centos.org/docs//4/4.5/Security_Guide/s2-ids-types.html*>, 28.10.2017 tarihinde erişildi.

[8] **Juan M. Estevez-Tapiador, Pedro Garcia-Teodoro, Jesus E. Diaz-Verdejo** (2004) Anomaly detection methods in wired networks: a survey and taxonomy.

[9] **Asieh Mokarian, Ahmad Faraahi, Arash Ghorbannia Delavar** (2013) False Positives Reduction Techniques in Intrusion Detection Systems-A Review, IJCSNS International Journal of Computer Science and Network 128 Security, VOL.13 No.10, October 2013.

[10] **M. E. Elhamahmy, Hesham N. Elmahdy and Imane A. Saroit** (2010) A New Approach for Evaluating Intrusion Detection System, CiiT International Journal of Artificial Intelligent Systems and Machine Learning, Vol 2, No 11, November 2010.

[11] **International Telecommunication Union (ITU)** (2017) Global Cybersecurity Index (GCI) 2017, ISBN 978-92-61-25071-3 (electronic version).

[12] **Saman Shojae Chaeikar, Mohammadreza Jafari, Hamed Taherdoost, Nakisa Shojae Chaei kar** (2012) Definitions and Criteria of CIA Security Triangle in Electronic Voting System, International Journal of Advanced Computer Science and Information Technology (IJACSIT) Vol. 1, No.1, October 2012, Page: 14-24, ISSN: 2296-1739.

[13] **Yuan Ho, Deborah Frincke, Donald Tobin, Jr** (1998) Planning, Petri Nets, and Intrusion Detection.

[14] **Ramazan Karademir** (2015) Intelligent Anomaly Detection Techniques for Denial of Service Attacks, Master of Science Thesis, The Republic of Turkey, Bahcesehir University.

[15] **URL-2** <*https://www.incapsula.com/ddos/ddos-attacks/*>, 28.10.2017 tarihinde erişildi.

[16] **Seong K, Narasimha R.** (2008) Statistical Techniques for Detecting Traffic anomalies through Packet Header Data, IEEE/ACM Transactions on Networking, vol. 16, no. 3, pp. 562, 575, Jun. 2008.

[17] **Bharanidharan Shanmugam and Norbik Bashah Idris** (2011) Hybrid Intrusion Detection Systems (HIDS) using Fuzzy Logic, Intrusion Detection Systems, ISBN 978-953-307-167-1.

[18] **Ye Nong, Masum Emran Syed, Chen Qiang, Vilbert Sean** (2002). Multivariate Statistical Analysis of Audit Trails for Host-Based Intrusion Detection. IEEE Trans. Computers. 51. 810-820.

[19] **Robert G. Gallager** (2013) Stochastic Processes: Theory for Applications, Chapter 2 Poisson Processes.

[20] **Cyriac James** (2012) Relevance of Time Series Models in Network Traffic Modeling: In The Context of TCP SYN DOS Attack, Master of Science Thesis, Department of Computer Science and Engineering Indian Institute of Technology Madras.

[21] **Sumit More, Mary Matthews, Anupam Joshi, Tim Finin** (2012) A Knowledge-Based Approach To Intrusion Detection Modeling.

[22] **Koral Ilgun, Richard A. Kemmerer, Fellow, IEEE, and Phillip A. Porras** (1995) State Transition Analysis: A Rule-Based Intrusion Detection Approach.

[23] **Abhinav S. Raut, Kavita R. Singh** (2014) Anomaly Based Intrusion Detection-A Review, Int. J. on Network Security, Vol. 5, 2014.

[24] **Ramazan Gençay** (1996) Non-linear Prediction of Security Returns with Moving Average Rules, University of Windsor, Canada, Journal of Forecasting, Vol. 15, 165-174 (1996).

[25] **Chao-Hui Yeh** (2012) The Profitability of Moving Average in Taiwan: A New Anomaly, International Journal of Business and Social Science Vol. 3 No. 20 [Special Issue – October 2012].

[26] **Shou Hsing Shih, Chris P. Tsokos** (2008) A Weighted Moving Average Process for Forecasting, Journal of Modern Applied Statistical Methods, May, 2008, Vol. 7, No. 1, 187-197.

[27] **Andreas Eckner** (2017) Algorithms for Unevenly Spaced Time Series: Moving Averages and Other Rolling Operators.

[28] **The National Institute of Standards and Technology (NIST) U.S. Department of Commerce** (2012) Engineering Statistics Handbook, 6.3.2.4. EWMA Control Charts.

[29] **Url-3** <*https://www.alanhull.com/hull-moving-average*>, 28.10.2017 tarihinde erişildi.

[30] **Valeriy Zakamulin** (2017) Market Timing with Moving Averages: The Anatomy and Performance of Trading Rules.

[31] **Laurent Dami** (1991) More Functional Reusability in C / C++ / Objective-c with Curried Functions, Centre Universitaire d'Informatique, University of Geneva, pp. 85-98, June 1991.

[32] **Ulisses Mello, Ildar Khabibrakhmanov** (2003) On the Reusability and Numeric Efficiency of C++ Packages in Scientific Computing, Proceedings of the ClusterWorld Conference and Expo, 2003.

[33] **Url-4** <*https://www.gnu.org/*>, 28.10.2017 tarihinde erişildi.

[34] **Url-5** <*https://packages.debian.org/jessie/g++*>, 28.10.2017 tarihinde erişildi.

[35] **Url-6** <*https://github.com/the-tcpdump-group/libpcap/blob/master/pcap/pcap.h*>, 28.10.2017 tarihinde erişildi.

[36] **Anna L. Buczak, Member, IEEE, and Erhan Guven, Member, IEEE** (2016) A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, IEEE Communications Surveys & Tutorials, VOL. 18, NO. 2, Second Quarter 2016.

[37] **Url-7** <https://www.iso.org/standard/20269.html>, 28.10.2017 tarihinde erişildi.

[38] **Url-8** <https://tools.ietf.org/html/rfc1122>, 28.10.2017 tarihinde erişildi.

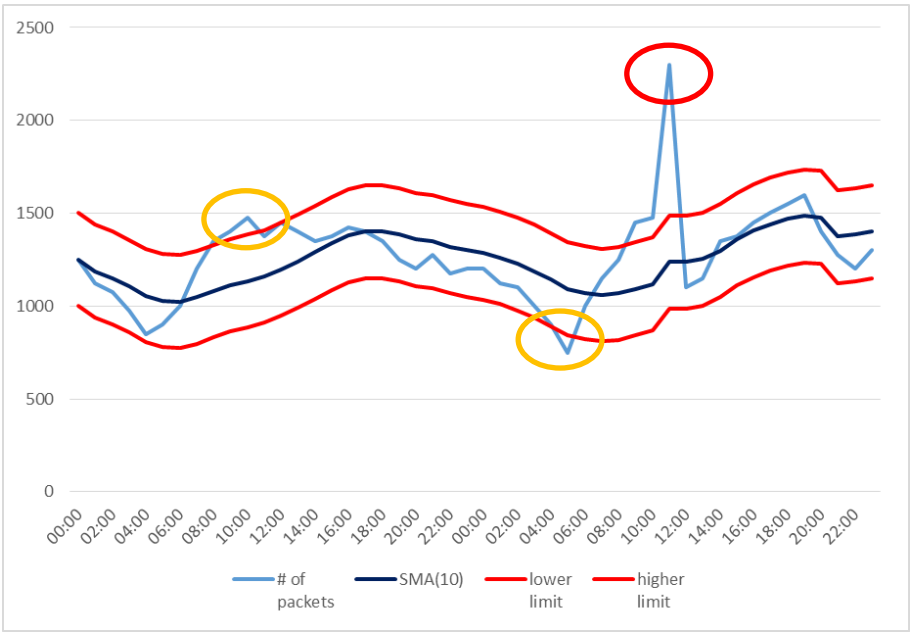
EKLER

EK A.1 $SMA_{(10)}$ Örneği

$$SMA(10) = \frac{(1275 + 1200 + 1250 + 1350 + 1400 + 1425 + 1375 + \cdots + 1450)}{10}$$
$$= \frac{13475}{10} = 1347{,}5 \qquad \pm 250 \text{ eşik değeri olarak seçilmiştir.}$$

Çizelge A.1 : $SMA_{(10)}$ Hesaplama Sonuç Tablosu

1. Gün	# Paket	SMA(10)	Alt Eşik	Üst Eşik		2. Gün	# Paket	SMA(10)	Alt Eşik	Üst Eşik
00:00	1250	1250	1000	1500		00:00	1200	1285	1035	1535
01:00	1125	1187,5	937,5	1437,5		01:00	1125	1260	1010	1510
02:00	1075	1150	900	1400		02:00	1100	1227,5	977,5	1477,5
03:00	975	1106,25	856,25	1356,3		03:00	1000	1187,5	937,5	1437,5
04:00	850	1055	805	1305		04:00	900	1142,5	892,5	1392,5
05:00	900	1029,167	779,17	1279,2		05:00	750	1092,5	842,5	1342,5
06:00	1000	1025	775	1275		06:00	1000	1072,5	822,5	1322,5
07:00	1200	1046,875	796,88	1296,9		07:00	1150	1060	810	1310
08:00	1350	1080,556	830,56	1330,6		08:00	1250	1067,5	817,5	1317,5
09:00	1400	1112,5	862,5	1362,5		09:00	1450	1092,5	842,5	1342,5
10:00	1475	1135	885	1385		10:00	1475	1120	870	1370
11:00	1375	1160	910	1410		11:00	2300	1237,5	987,5	1487,5
12:00	1450	1197,5	947,5	1447,5		12:00	1100	1237,5	987,5	1487,5
13:00	1400	1240	990	1490		13:00	1150	1252,5	1002,5	1502,5
14:00	1350	1290	1040	1540		14:00	1350	1297,5	1047,5	1547,5
15:00	1375	1337,5	1087,5	1587,5		15:00	1375	1360	1110	1610
16:00	1425	1380	1130	1630		16:00	1450	1405	1155	1655
17:00	1400	1400	1150	1650		17:00	1500	1440	1190	1690
18:00	1350	1400	1150	1650		18:00	1550	1470	1220	1720
19:00	1250	1385	1135	1635		19:00	1600	1485	1235	1735
20:00	1200	1357,5	1107,5	1607,5		20:00	1400	1477,5	1227,5	1727,5
21:00	1275	1347,5	1097,5	1597,5		21:00	1275	1375	1125	1625
22:00	1175	1320	1070	1570		22:00	1200	1385	1135	1635
23:00	1200	1300	1050	1550		23:00	1300	1400	1150	1650



Şekil A.1 : $SMA_{(10)}$ Analiz Sonucu

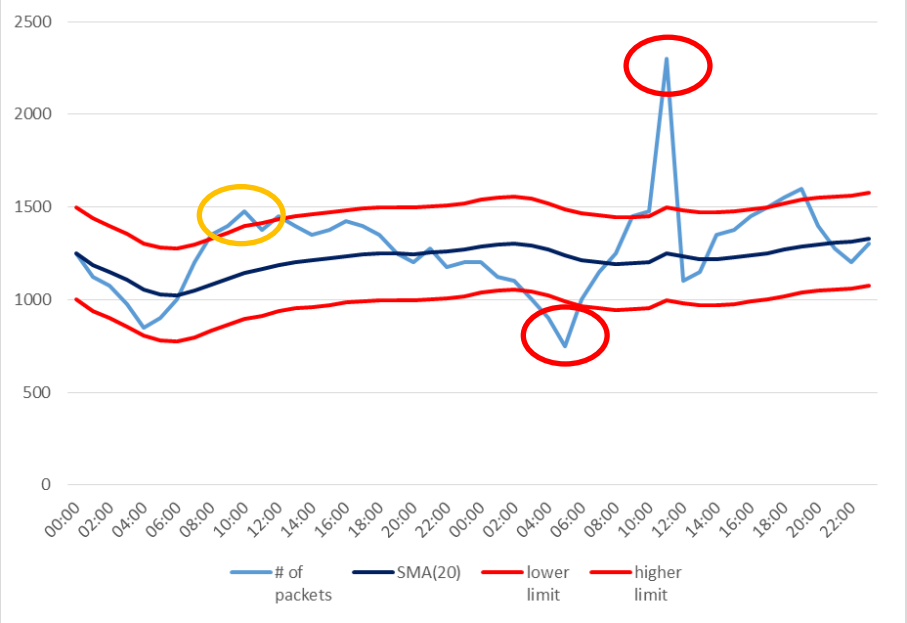
EK A.2 $SMA_{(20)}$ Örneği

$$SMA(20) = \frac{(1275 + 1200 + 1250 + 1350 + 1400 + 1425 + 1375 + \cdots + 1075)}{20}$$

$$= \frac{25075}{20} = 1253{,}75 \qquad \pm 250 \text{ eşik değeri olarak seçilmiştir.}$$

Çizelge A.2 : $SMA_{(20)}$ Hesaplama Sonuç Tablosu

1. Gün	# Paket	SMA(10)	Alt Eşik	Üst Eşik	2. Gün	# Paket	SMA(10)	Alt Eşik	Üst Eşik
00:00	1250	1250	1000	1500	00:00	1200	1287,5	1037,5	1537,5
01:00	1125	1187,5	937,5	1437,5	01:00	1125	1298,75	1048,8	1548,8
02:00	1075	1150	900	1400	02:00	1100	1303,75	1053,8	1553,8
03:00	975	1106,25	856,25	1356,3	03:00	1000	1293,75	1043,8	1543,8
04:00	850	1055	805	1305	04:00	900	1271,25	1021,3	1521,3
05:00	900	1029,167	779,17	1279,2	05:00	750	1238,75	988,75	1488,8
06:00	1000	1025	775	1275	06:00	1000	1215	965	1465
07:00	1200	1046,875	796,88	1296,9	07:00	1150	1203,75	953,75	1453,8
08:00	1350	1080,556	830,56	1330,6	08:00	1250	1193,75	943,75	1443,8
09:00	1400	1112,5	862,5	1362,5	09:00	1450	1196,25	946,25	1446,3
10:00	1475	1145,455	895,45	1395,5	10:00	1475	1202,5	952,5	1452,5
11:00	1375	1164,583	914,58	1414,6	11:00	2300	1248,75	998,75	1498,8
12:00	1450	1186,538	936,54	1436,5	12:00	1100	1232,5	982,5	1482,5
13:00	1400	1201,786	951,79	1451,8	13:00	1150	1220	970	1470
14:00	1350	1211,667	961,67	1461,7	14:00	1350	1220	970	1470
15:00	1375	1221,875	971,88	1471,9	15:00	1375	1226,25	976,25	1476,3
16:00	1425	1233,824	983,82	1483,8	16:00	1450	1238,75	988,75	1488,8
17:00	1400	1243,056	993,06	1493,1	17:00	1500	1250	1000	1500
18:00	1350	1248,684	998,68	1498,7	18:00	1550	1268,75	1018,8	1518,8
19:00	1250	1248,75	998,75	1498,8	19:00	1600	1288,75	1038,8	1538,8
20:00	1200	1246,25	996,25	1496,3	20:00	1400	1298,75	1048,8	1548,8
21:00	1275	1253,75	1003,8	1503,8	21:00	1275	1306,25	1056,3	1556,3
22:00	1175	1258,75	1008,8	1508,8	22:00	1200	1311,25	1061,3	1561,3
23:00	1200	1270	1020	1520	23:00	1300	1326,25	1076,3	1576,3



Şekil A.2 : $SMA_{(20)}$ Analiz Sonucu

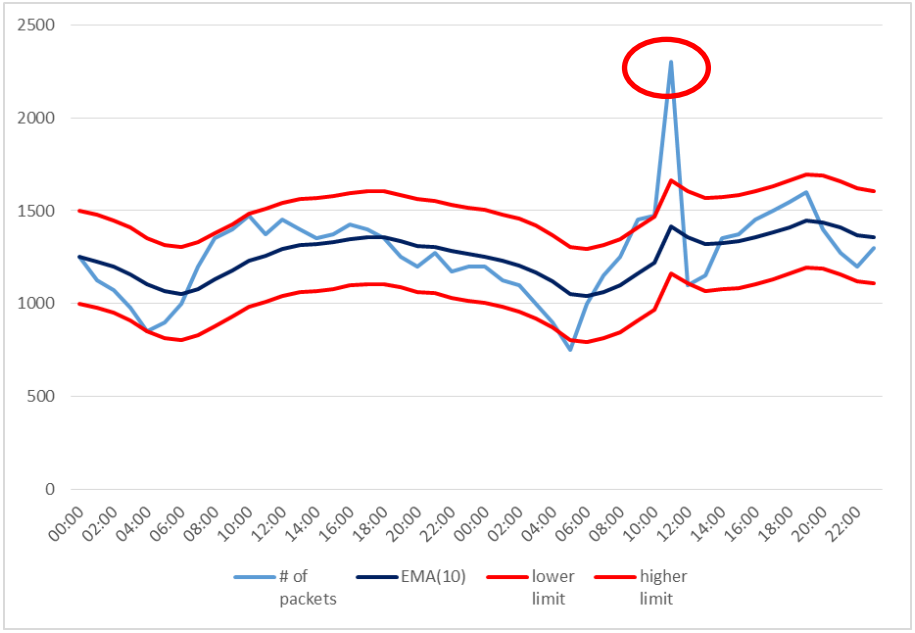
EK A.3 $EMA_{(10)}$ Örneği

$\propto = \frac{2}{1+10} = 0,\overline{18}$ $\pm$ 250 eşik değeri olarak seçilmiştir.

$EMA_{10} = ((1350 - 1355,36) * 0,18) + 1355,36 = 1336,21$

Çizelge A.3 : $EMA_{(10)}$ Hesaplama Sonuç Tablosu

1. Gün	# Paket	EMA(10)	Alt Eşik	Üst Eşik	2. Gün	# Paket	EMA(10)	Alt Eşik	Üst Eşik
00:00	1250	1250,00	1000,00	1500,00	00:00	1200	1254,37	1004,37	1504,37
01:00	1125	1227,27	977,27	1477,27	01:00	1125	1230,84	980,84	1480,84
02:00	1075	1199,59	949,59	1449,59	02:00	1100	1207,05	957,05	1457,05
03:00	975	1158,75	908,75	1408,75	03:00	1000	1169,41	919,41	1419,41
04:00	850	1102,62	852,62	1352,62	04:00	900	1120,43	870,43	1370,43
05:00	900	1065,78	815,78	1315,78	05:00	750	1053,08	803,08	1303,08
06:00	1000	1053,82	803,82	1303,82	06:00	1000	1043,43	793,43	1293,43
07:00	1200	1080,40	830,40	1330,40	07:00	1150	1062,80	812,80	1312,80
08:00	1350	1129,41	879,41	1379,41	08:00	1250	1096,84	846,84	1346,84
09:00	1400	1178,61	928,61	1428,61	09:00	1450	1161,05	911,05	1411,05
10:00	1475	1232,50	982,50	1482,50	10:00	1475	1218,13	968,13	1468,13
11:00	1375	1258,41	1008,41	1508,41	11:00	2300	1414,83	1164,83	1664,83
12:00	1450	1293,24	1043,24	1543,24	12:00	1100	1357,59	1107,59	1607,59
13:00	1400	1312,65	1062,65	1562,65	13:00	1150	1319,85	1069,85	1569,85
14:00	1350	1319,44	1069,44	1569,44	14:00	1350	1325,33	1075,33	1575,33
15:00	1375	1329,55	1079,55	1579,55	15:00	1375	1334,36	1084,36	1584,36
16:00	1425	1346,90	1096,90	1596,90	16:00	1450	1355,39	1105,39	1605,39
17:00	1400	1356,56	1106,56	1606,56	17:00	1500	1381,68	1131,68	1631,68
18:00	1350	1355,36	1105,36	1605,36	18:00	1550	1412,28	1162,28	1662,28
19:00	1250	1336,21	1086,21	1586,21	19:00	1600	1446,41	1196,41	1696,41
20:00	1200	1311,44	1061,44	1561,44	20:00	1400	1437,97	1187,97	1687,97
21:00	1275	1304,82	1054,82	1554,82	21:00	1275	1408,34	1158,34	1658,34
22:00	1175	1281,21	1031,21	1531,21	22:00	1200	1370,46	1120,46	1620,46
23:00	1200	1266,45	1016,45	1516,45	23:00	1300	1357,65	1107,65	1607,65



Şekil A.3 : $EMA_{(10)}$ Analiz Sonucu

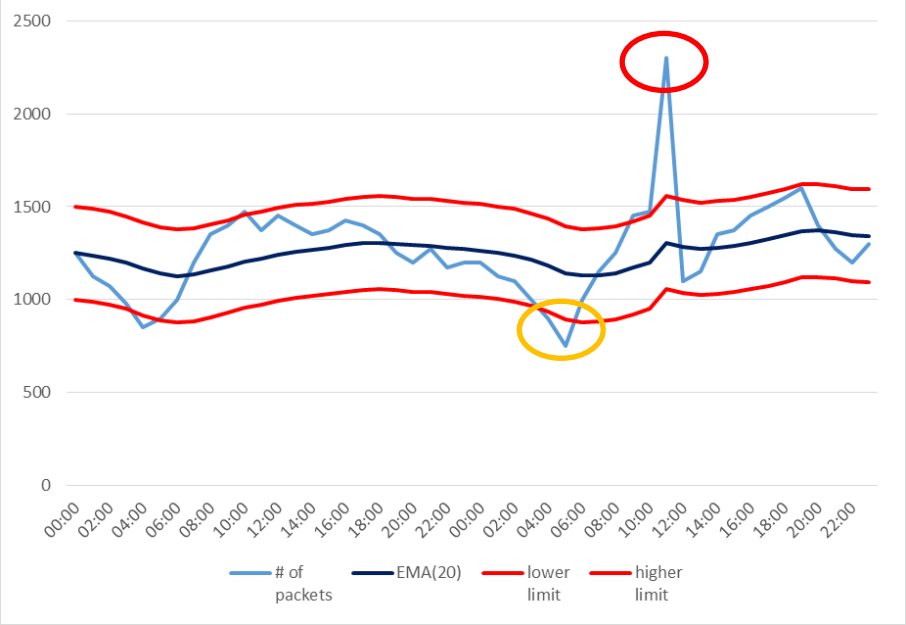
EK A.4 $EMA_{(20)}$ Örneği

$$\propto = \frac{2}{1+20} = 0{,}09523 \qquad \pm 250 \text{ eşik değeri olarak seçilmiştir.}$$

$$EMA_{20} = ((1350 - 1306{,}661) * 0{,}09523) + 1306{,}661 = 1301{,}265$$

Çizelge A.4 : $EMA_{(20)}$ Hesaplama Sonuç Tablosu

1. Gün	# Paket	EMA(20)	Alt Eşik	Üst Eşik	2. Gün	# Paket	EMA(20)	Alt Eşik	Üst Eşik
00:00	1250	1250	1000	1500	00:00	1200	1264,736	1014,7	1514,7
01:00	1125	1238,095	988,1	1488,1	01:00	1125	1251,428	1001,4	1501,4
02:00	1075	1222,562	972,56	1472,6	02:00	1100	1237,006	987,01	1487
03:00	975	1198,985	948,98	1449	03:00	1000	1214,434	964,43	1464,4
04:00	850	1165,748	915,75	1415,7	04:00	900	1184,488	934,49	1434,5
05:00	900	1140,439	890,44	1390,4	05:00	750	1143,108	893,11	1393,1
06:00	1000	1127,064	877,06	1377,1	06:00	1000	1129,479	879,48	1379,5
07:00	1200	1134,01	884,01	1384	07:00	1150	1131,433	881,43	1381,4
08:00	1350	1154,581	904,58	1404,6	08:00	1250	1142,725	892,73	1392,7
09:00	1400	1177,954	927,95	1428	09:00	1450	1171,989	921,99	1422
10:00	1475	1206,244	956,24	1456,2	10:00	1475	1200,848	950,85	1450,8
11:00	1375	1222,316	972,32	1472,3	11:00	2300	1305,529	1055,5	1555,5
12:00	1450	1244	994	1494	12:00	1100	1285,955	1036	1536
13:00	1400	1258,857	1008,9	1508,9	13:00	1150	1273,007	1023	1523
14:00	1350	1267,538	1017,5	1517,5	14:00	1350	1280,339	1030,3	1530,3
15:00	1375	1277,772	1027,8	1527,8	15:00	1375	1289,355	1039,4	1539,4
16:00	1425	1291,794	1041,8	1541,8	16:00	1450	1304,654	1054,7	1554,7
17:00	1400	1302,099	1052,1	1552,1	17:00	1500	1323,259	1073,3	1573,3
18:00	1350	1306,661	1056,7	1556,7	18:00	1550	1344,853	1094,9	1594,9
19:00	1250	1301,265	1051,3	1551,3	19:00	1600	1369,153	1119,2	1619,2
20:00	1200	1291,621	1041,6	1541,6	20:00	1400	1372,091	1122,1	1622,1
21:00	1275	1290,038	1040	1540	21:00	1275	1362,844	1112,8	1612,8
22:00	1175	1279,082	1029,1	1529,1	22:00	1200	1347,335	1097,3	1597,3
23:00	1200	1271,55	1021,6	1521,6	23:00	1300	1342,827	1092,8	1592,8



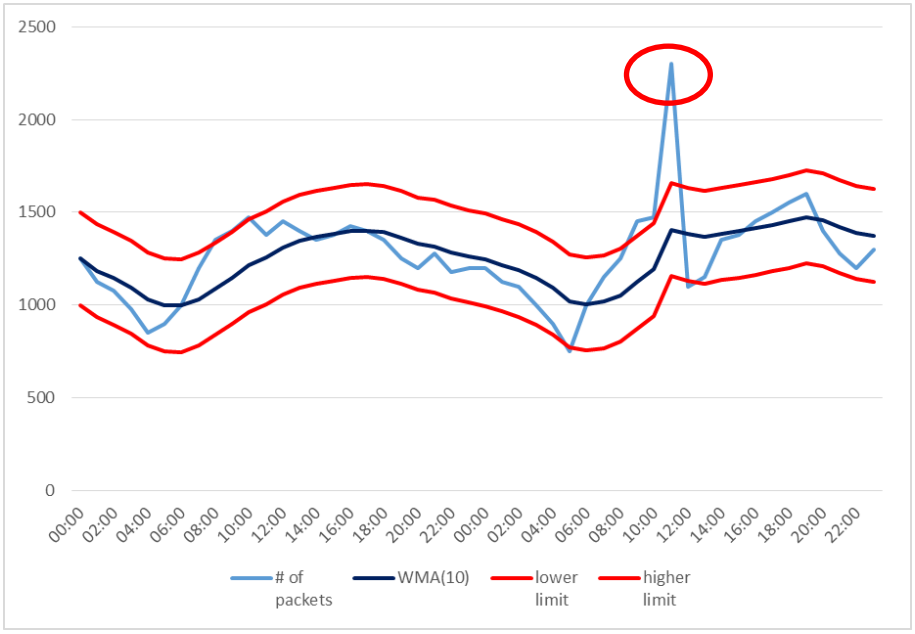
Şekil A.4 : $EMA_{(20)}$ Analiz Sonucu

EK A.5 $WMA_{(10)}$ Örneği

$$WMA(10) = \frac{(1275 * 10) + (1200 * 9) + (1250 * 8) + (1350 * 7) + \cdots + (1450 * 1)}{55}$$
$$= \frac{72325}{55} = 1315 \qquad \pm 250 \text{ eşik değeri olarak seçilmiştir.}$$

Çizelge A.5 : $WMA_{(10)}$ Hesaplama Sonuç Tablosu

1. Gün	# Paket	WMA(10)	Alt Eşik	Üst Eşik		2. Gün	# Paket	WMA(10)	Alt Eşik	Üst Eşik
00:00	1250	1250	1000	1500		00:00	1200	1243,636	993,64	1493,6
01:00	1125	1184,211	934,21	1434,2		01:00	1125	1214,545	964,55	1464,5
02:00	1075	1143,519	893,52	1393,5		02:00	1100	1185,455	935,45	1435,5
03:00	975	1093,382	843,38	1343,4		03:00	1000	1144,091	894,09	1394,1
04:00	850	1031,25	781,25	1281,3		04:00	900	1091,818	841,82	1341,8
05:00	900	999,4444	749,44	1249,4		05:00	750	1020,455	770,45	1270,5
06:00	1000	995,9184	745,92	1245,9		06:00	1000	1003,636	753,64	1253,6
07:00	1200	1031,25	781,25	1281,3		07:00	1150	1017,727	767,73	1267,7
08:00	1350	1087,963	837,96	1338		08:00	1250	1052,273	802,27	1302,3
09:00	1400	1145,909	895,91	1395,9		09:00	1450	1121,818	871,82	1371,8
10:00	1475	1211,818	961,82	1461,8		10:00	1475	1191,364	941,36	1441,4
11:00	1375	1255,455	1005,5	1505,5		11:00	2300	1405,909	1155,9	1655,9
12:00	1450	1308,182	1058,2	1558,2		12:00	1100	1380,909	1130,9	1630,9
13:00	1400	1345	1095	1595		13:00	1150	1365	1115	1615
14:00	1350	1365	1115	1615		14:00	1350	1382,727	1132,7	1632,7
15:00	1375	1380,455	1130,5	1630,5		15:00	1375	1396,818	1146,8	1646,8
16:00	1425	1396,364	1146,4	1646,4		16:00	1450	1413,182	1163,2	1663,2
17:00	1400	1400	1150	1650		17:00	1500	1430,455	1180,5	1680,5
18:00	1350	1390,909	1140,9	1640,9		18:00	1550	1450,455	1200,5	1700,5
19:00	1250	1363,636	1113,6	1613,6		19:00	1600	1474,091	1224,1	1724,1
20:00	1200	1330	1080	1580		20:00	1400	1458,636	1208,6	1708,6
21:00	1275	1315	1065	1565		21:00	1275	1421,818	1171,8	1671,8
22:00	1175	1283,636	1033,6	1533,6		22:00	1200	1390	1140	1640
23:00	1200	1261,818	1011,8	1511,8		23:00	1300	1374,545	1124,5	1624,5



Şekil A.5 : $WMA_{(10)}$ Analiz Sonucu

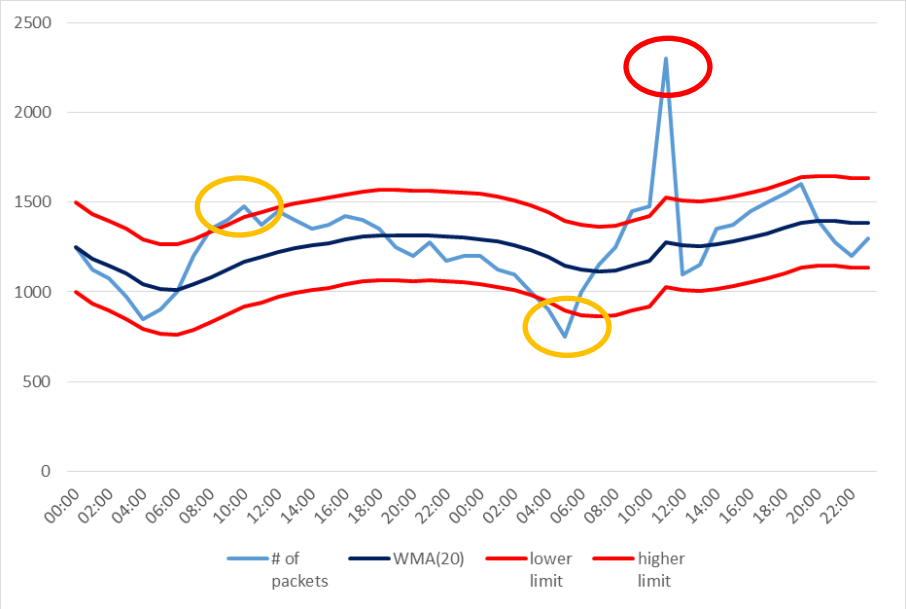
EK A.6 $WMA_{(20)}$ Örneği

$$WMA(20) = \frac{(1275 * 20) + (1200 * 19) + (1250 * 18) + (1350 * 17) + \cdots + (1075 * 1)}{210}$$

$$= \frac{276125}{210} = 1314{,}881 \qquad \pm 250 \text{ eşik değeri olarak seçilmiştir.}$$

Çizelge A.6 : $WMA_{(20)}$ Hesaplama Sonuç Tablosu

1. Gün	# Paket	WMA(20)	Alt Eşik	Üst Eşik	2. Gün	# Paket	WMA(20)	Alt Eşik	Üst Eşik
00:00	1250	1250	1000	1500	00:00	1200	1295,119	1045,1	1545,1
01:00	1125	1185,897	935,9	1435,9	01:00	1125	1279,643	1029,6	1529,6
02:00	1075	1146,93	896,93	1396,9	02:00	1100	1260,714	1010,7	1510,7
03:00	975	1100,338	850,34	1350,3	03:00	1000	1231,786	981,79	1481,8
04:00	850	1044,444	794,44	1294,4	04:00	900	1194,286	944,29	1444,3
05:00	900	1016,429	766,43	1266,4	05:00	750	1144,643	894,64	1394,6
06:00	1000	1013,025	763,03	1263	06:00	1000	1121,905	871,9	1371,9
07:00	1200	1040,72	790,72	1290,7	07:00	1150	1115,714	865,71	1365,7
08:00	1350	1083,333	833,33	1333,3	08:00	1250	1120,119	870,12	1370,1
09:00	1400	1124,355	874,35	1374,4	09:00	1450	1144,524	894,52	1394,5
10:00	1475	1167,576	917,58	1417,6	10:00	1475	1171,071	921,07	1421,1
11:00	1375	1192,816	942,82	1442,8	11:00	2300	1275,595	1025,6	1525,6
12:00	1450	1222,94	972,94	1472,9	12:00	1100	1261,429	1011,4	1511,4
13:00	1400	1244,18	994,18	1494,2	13:00	1150	1253,571	1003,6	1503,6
14:00	1350	1258,077	1008,1	1508,1	14:00	1350	1265,952	1016	1516
15:00	1375	1273,25	1023,3	1523,3	15:00	1375	1280,714	1030,7	1530,7
16:00	1425	1292,157	1042,2	1542,2	16:00	1450	1302,024	1052	1552
17:00	1400	1307,367	1057,4	1557,4	17:00	1500	1326,905	1076,9	1576,9
18:00	1350	1316,986	1067	1567	18:00	1550	1355,476	1105,5	1605,5
19:00	1250	1316,786	1066,8	1566,8	19:00	1600	1387,024	1137	1637
20:00	1200	1312,143	1062,1	1562,1	20:00	1400	1397,619	1147,6	1647,6
21:00	1275	1314,881	1064,9	1564,9	21:00	1275	1395,357	1145,4	1645,4
22:00	1175	1307,381	1057,4	1557,4	22:00	1200	1385,238	1135,2	1635,2
23:00	1200	1301,786	1051,8	1551,8	23:00	1300	1384,167	1134,2	1634,2



Şekil A.6 : $WMA_{(20)}$ Analiz Sonucu

EK A.7 $HMA_{(10)}$ Örneği

$$WMA(10) = \frac{(1275 * 10) + (1200 * 9) + (1250 * 8) + (1350 * 7) + \cdots + (1450 * 1)}{55}$$

$$= \frac{72325}{55} = 1315$$

$$2 * WMA(5) = \frac{(1275 * 5) + (1200 * 4) + (1250 * 3) + (1350 * 2) + (1400 * 1)}{15}$$

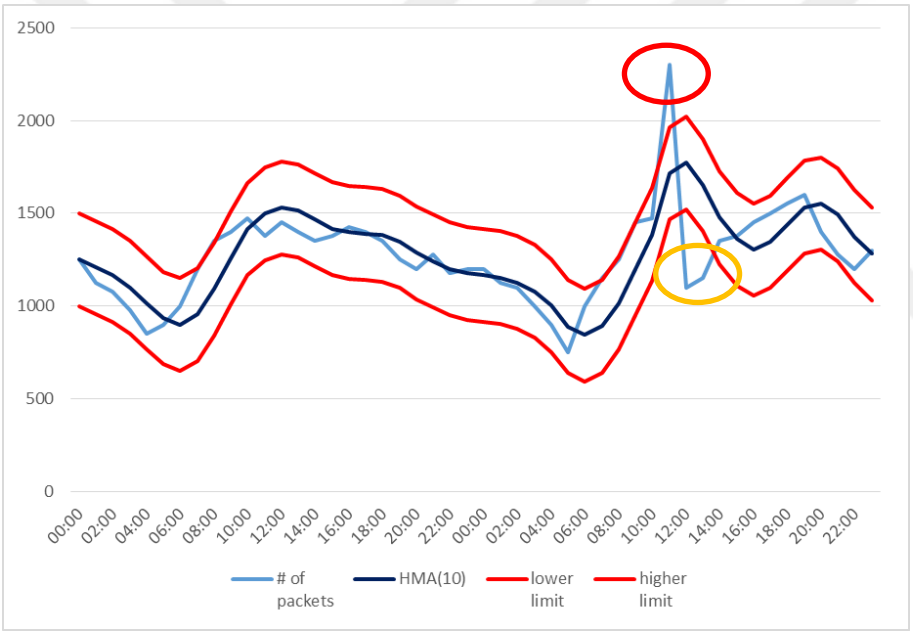
$$= 2 * \frac{19025}{15} = 2536{,}67$$

$$d = \left(2 * WMA(5) - WMA(10)\right)$$

d dizisi için; $HMA(10) = WMA\left(\sqrt{10}\right) \cong WMA(3)$ *olur*.

WMA(3) hesaplanarak HMA(10) bulunur.

± 250 *eşik değeri olarak seçilmiştir*.



Şekil A.7 : HMA(10) Analiz Sonucu

Çizelge A.7 : $HMA_{(10)}$ Hesaplama Sonuç Tablosu

1. Gün	# Paket	WMA(10)	2*WMA(5)	d	HMA(10)	Alt Eşik	Üst Eşik
00:00	1250	1250,00	2500,00	1250,00	1250,00	1000,00	1500,00
01:00	1125	1184,21	2361,11	1176,90	1206,14	956,14	1456,14
02:00	1075	1143,52	2270,83	1127,31	1164,29	914,29	1414,29
03:00	975	1093,38	2150,00	1056,62	1100,23	850,23	1350,23
04:00	850	1031,25	1983,33	952,08	1016,13	766,13	1266,13
05:00	900	999,44	1880,00	880,56	933,74	683,74	1183,74
06:00	1000	995,92	1890,00	894,08	899,24	649,24	1149,24
07:00	1200	1031,25	2050,00	1018,75	954,16	704,16	1204,16
08:00	1350	1087,96	2293,33	1205,37	1091,28	841,28	1341,28
09:00	1400	1145,91	2520,00	1374,09	1258,63	1008,63	1508,63
10:00	1475	1211,82	2723,33	1511,52	1414,68	1164,68	1664,68
11:00	1375	1255,45	2783,33	1527,88	1496,79	1246,79	1746,79
12:00	1450	1308,18	2843,33	1535,15	1528,79	1278,79	1778,79
13:00	1400	1345,00	2836,67	1491,67	1512,20	1262,20	1762,20
14:00	1350	1365,00	2790,00	1425,00	1465,58	1215,58	1715,58
15:00	1375	1380,45	2766,67	1386,21	1416,72	1166,72	1666,72
16:00	1425	1396,36	2790,00	1393,64	1396,39	1146,39	1646,39
17:00	1400	1400,00	2790,00	1390,00	1390,58	1140,58	1640,58
18:00	1350	1390,91	2763,33	1372,42	1381,82	1131,82	1631,82
19:00	1250	1363,64	2676,67	1313,03	1345,66	1095,66	1595,66
20:00	1200	1330,00	2570,00	1240,00	1286,41	1036,41	1536,41
21:00	1275	1315,00	2536,67	1221,67	1243,01	993,01	1493,01
22:00	1175	1283,64	2456,67	1173,03	1200,40	950,40	1450,40
23:00	1200	1261,82	2423,33	1161,52	1175,38	925,38	1425,38
2. Gün	# Paket	WMA(10)	2*WMA(5)	d	HMA(10)	Alt Eşik	Üst Eşik
00:00	1200	1243,64	2410,00	1166,36	1165,86	915,86	1415,86
01:00	1125	1214,55	2353,33	1138,79	1151,77	901,77	1401,77
02:00	1100	1185,45	2290,00	1104,55	1126,26	876,26	1376,26
03:00	1000	1144,09	2183,33	1039,24	1077,60	827,60	1327,60
04:00	900	1091,82	2033,33	941,52	1001,26	751,26	1251,26
05:00	750	1020,45	1823,33	802,88	888,48	638,48	1138,48
06:00	1000	1003,64	1840,00	836,36	842,73	592,73	1092,73
07:00	1150	1017,73	1973,33	955,61	890,40	640,40	1140,40
08:00	1250	1052,27	2166,67	1114,39	1015,13	765,13	1265,13
09:00	1450	1121,82	2460,00	1338,18	1199,82	949,82	1449,82
10:00	1475	1191,36	2696,67	1505,30	1384,44	1134,44	1634,44
11:00	2300	1405,91	3386,67	1980,76	1715,18	1465,18	1965,18
12:00	1100	1380,91	3103,33	1722,42	1772,35	1522,35	2022,35
13:00	1150	1365,00	2860,00	1495,00	1651,77	1401,77	1901,77
14:00	1350	1382,73	2763,33	1380,61	1475,71	1225,71	1725,71
15:00	1375	1396,82	2696,67	1299,85	1359,29	1109,29	1609,29
16:00	1450	1413,18	2693,33	1280,15	1303,46	1053,46	1553,46
17:00	1500	1430,45	2836,67	1406,21	1346,46	1096,46	1596,46
18:00	1550	1450,45	2960,00	1509,55	1436,87	1186,87	1686,87
19:00	1600	1474,09	3063,33	1589,24	1532,17	1282,17	1782,17
20:00	1400	1458,64	3000,00	1541,36	1552,02	1302,02	1802,02
21:00	1275	1421,82	2850,00	1428,18	1492,75	1242,75	1742,75
22:00	1200	1390,00	2673,33	1283,33	1374,62	1124,62	1624,62
23:00	1300	1374,55	2603,33	1228,79	1280,20	1030,20	1530,20

EK A.8 $HMA_{(20)}$ Örneği

$$WMA(20) = \frac{(1275 * 20) + (1200 * 19) + (1250 * 18) + (1350 * 17) + \cdots + (1075 * 1)}{210}$$

$$= \frac{276125}{210} = 1314{,}88$$

$$2 * WMA(10) = \frac{(1275 * 10) + (1200 * 9) + (1250 * 8) + (1350 * 7) + \cdots + (1450 * 1)}{55}$$

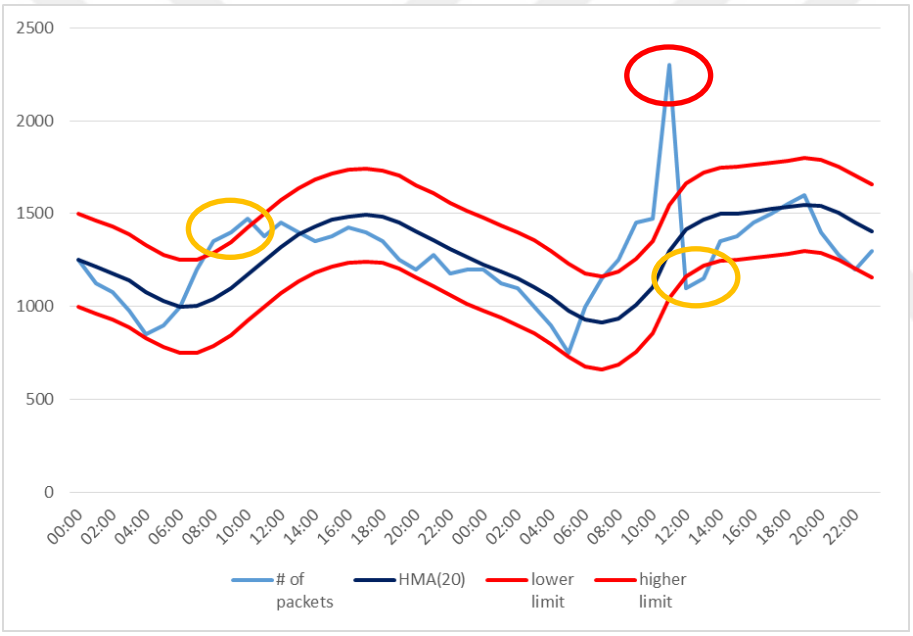
$$= 2 * \frac{72325}{55} = 2630$$

$$d = \left(2 * WMA(10) - WMA(20)\right)$$

d dizisi için; $HMA(20) = WMA\left(\sqrt{20}\right) \cong WMA(4)$

WMA(4) hesaplanarak HMA(20) bulunur.

± 250 *eşik değeri olarak seçilmiştir.*



Şekil A.8 : HMA(20) Analiz Sonucu

Çizelge A.8 : $HMA_{(20)}$ Hesaplama Sonuç Tablosu

1. Gün	# Paket	WMA(20)	2*WMA(10)	d	HMA(20)	Alt Eşik	Üst Eşik
00:00	1250	1250,00	2500,00	1250,00	1250,00	1000,00	1500,00
01:00	1125	1185,90	2368,42	1182,52	1211,44	961,44	1461,44
02:00	1075	1146,93	2287,04	1140,11	1178,67	928,67	1428,67
03:00	975	1100,34	2186,76	1086,43	1138,11	888,11	1388,11
04:00	850	1044,44	2062,50	1018,06	1079,42	829,42	1329,42
05:00	900	1016,43	1998,89	982,46	1029,70	779,70	1279,70
06:00	1000	1013,03	1991,84	978,81	998,52	748,52	1248,52
07:00	1200	1040,72	2062,50	1021,78	1000,65	750,65	1250,65
08:00	1350	1083,33	2175,93	1092,59	1037,58	787,58	1287,58
09:00	1400	1124,35	2291,82	1167,46	1097,00	847,00	1347,00
10:00	1475	1167,58	2423,64	1256,06	1173,36	923,36	1423,36
11:00	1375	1192,82	2510,91	1318,09	1246,81	996,81	1496,81
12:00	1450	1222,94	2616,36	1393,42	1320,76	1070,76	1570,76
13:00	1400	1244,18	2690,00	1445,82	1385,58	1135,58	1635,58
14:00	1350	1258,08	2730,00	1471,92	1433,01	1183,01	1683,01
15:00	1375	1273,25	2760,91	1487,66	1465,15	1215,15	1715,15
16:00	1425	1292,16	2792,73	1500,57	1485,49	1235,49	1735,49
17:00	1400	1307,37	2800,00	1492,63	1491,95	1241,95	1741,95
18:00	1350	1316,99	2781,82	1464,83	1482,60	1232,60	1732,60
19:00	1250	1316,79	2727,27	1410,49	1452,23	1202,23	1702,23
20:00	1200	1312,14	2660,00	1347,86	1404,52	1154,52	1654,52
21:00	1275	1314,88	2630,00	1315,12	1358,99	1108,99	1608,99
22:00	1175	1307,38	2567,27	1259,89	1309,11	1059,11	1559,11
23:00	1200	1301,79	2523,64	1221,85	1264,52	1014,52	1514,52
2. Gün	# Paket	WMA(20)	2*WMA(10)	d	HMA(20)	Alt Eşik	Üst Eşik
00:00	1200	1295,12	2487,27	1192,15	1226,91	976,91	1476,91
01:00	1125	1279,64	2429,09	1149,45	1187,78	937,78	1437,78
02:00	1100	1260,71	2370,91	1110,19	1149,53	899,53	1399,53
03:00	1000	1231,79	2288,18	1056,40	1104,72	854,72	1354,72
04:00	900	1194,29	2183,64	989,35	1049,64	799,64	1299,64
05:00	750	1144,64	2040,91	896,27	977,61	727,61	1227,61
06:00	1000	1121,90	2007,27	885,37	926,54	676,54	1176,54
07:00	1150	1115,71	2035,45	919,74	911,69	661,69	1161,69
08:00	1250	1120,12	2104,55	984,43	936,39	686,39	1186,39
09:00	1450	1144,52	2243,64	1099,11	1007,46	757,46	1257,46
10:00	1475	1171,07	2382,73	1211,66	1103,26	853,26	1353,26
11:00	2300	1275,60	2811,82	1536,22	1296,25	1046,25	1546,25
12:00	1100	1261,43	2761,82	1500,39	1413,27	1163,27	1663,27
13:00	1150	1253,57	2730,00	1476,43	1469,10	1219,10	1719,10
14:00	1350	1265,95	2765,45	1499,50	1496,43	1246,43	1746,43
15:00	1375	1280,71	2793,64	1512,92	1500,34	1250,34	1750,34
16:00	1450	1302,02	2826,36	1524,34	1511,16	1261,16	1761,16
17:00	1500	1326,90	2860,91	1534,00	1523,44	1273,44	1773,44
18:00	1550	1355,48	2900,91	1545,43	1534,53	1284,53	1784,53
19:00	1600	1387,02	2948,18	1561,16	1547,33	1297,33	1797,33
20:00	1400	1397,62	2917,27	1519,65	1538,70	1288,70	1788,70
21:00	1275	1395,36	2843,64	1448,28	1501,98	1251,98	1751,98
22:00	1200	1385,24	2780,00	1394,76	1452,44	1202,44	1702,44
23:00	1300	1384,17	2749,09	1364,92	1406,02	1156,02	1656,02

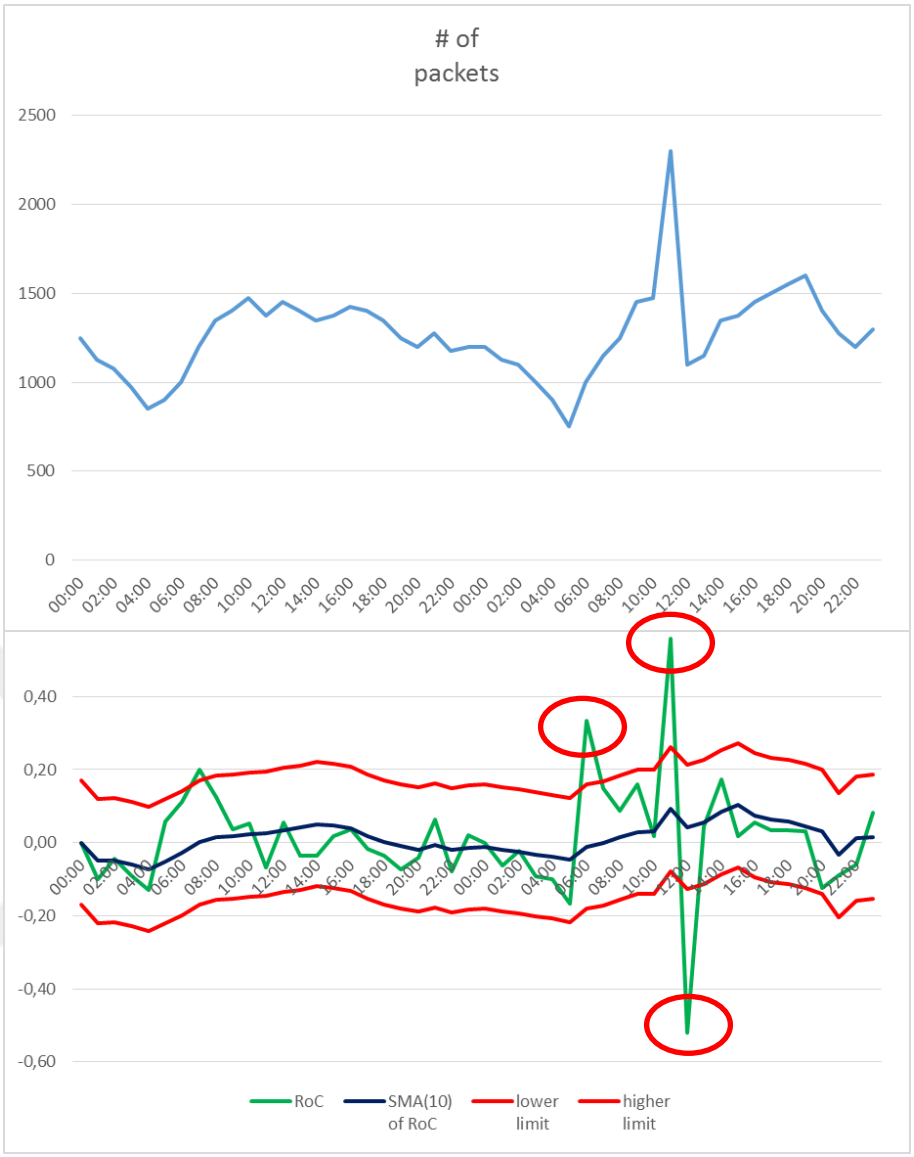
EK A.9 RoC Örneği

$RoC = \frac{1375}{1475} - 1 = -0{,}07$ hesaplanan bu dizinin SMA(10)değeri hesaplanmıştır.

$\pm 0{,}17$ eşik değeri olarak seçilmiştir.

Çizelge A.9 : RoC Hesaplama Sonuç Tablosu

1. Gün	# Paket	RoC	SMA(10) RoC	Alt Eşik	Üst Eşik		2. Gün	# Paket	RoC	SMA(10) RoC	Alt Eşik	Üst Eşik
00:00	1250	0,00	0,000	-0,170	0,170		00:00	1200	0,00	-0,011	-0,181	0,159
01:00	1125	-0,10	-0,050	-0,220	0,120		01:00	1125	-0,06	-0,019	-0,189	0,151
02:00	1075	-0,04	-0,048	-0,218	0,122		02:00	1100	-0,02	-0,025	-0,195	0,145
03:00	975	-0,09	-0,059	-0,229	0,111		03:00	1000	-0,09	-0,032	-0,202	0,138
04:00	850	-0,13	-0,073	-0,243	0,097		04:00	900	-0,10	-0,038	-0,208	0,132
05:00	900	0,06	-0,051	-0,221	0,119		05:00	750	-0,17	-0,048	-0,218	0,122
06:00	1000	0,11	-0,028	-0,198	0,142		06:00	1000	0,33	-0,010	-0,180	0,160
07:00	1200	0,20	0,001	-0,169	0,171		07:00	1150	0,15	-0,002	-0,172	0,168
08:00	1350	0,13	0,014	-0,156	0,184		08:00	1250	0,09	0,015	-0,155	0,185
09:00	1400	0,04	0,017	-0,153	0,187		09:00	1450	0,16	0,029	-0,141	0,199
10:00	1475	0,05	0,022	-0,148	0,192		10:00	1475	0,02	0,031	-0,139	0,201
11:00	1375	-0,07	0,025	-0,145	0,195		11:00	2300	0,56	0,093	-0,077	0,263
12:00	1450	0,05	0,035	-0,135	0,205		12:00	1100	-0,52	0,043	-0,127	0,213
13:00	1400	-0,03	0,041	-0,129	0,211		13:00	1150	0,05	0,056	-0,114	0,226
14:00	1350	-0,04	0,050	-0,120	0,220		14:00	1350	0,17	0,084	-0,086	0,254
15:00	1375	0,02	0,046	-0,124	0,216		15:00	1375	0,02	0,102	-0,068	0,272
16:00	1425	0,04	0,039	-0,131	0,209		16:00	1450	0,05	0,074	-0,096	0,244
17:00	1400	-0,02	0,017	-0,153	0,187		17:00	1500	0,03	0,063	-0,107	0,233
18:00	1350	-0,04	0,001	-0,169	0,171		18:00	1550	0,03	0,058	-0,112	0,228
19:00	1250	-0,07	-0,010	-0,180	0,160		19:00	1600	0,03	0,045	-0,125	0,215
20:00	1200	-0,04	-0,020	-0,190	0,150		20:00	1400	-0,13	0,031	-0,139	0,201
21:00	1275	0,06	-0,007	-0,177	0,163		21:00	1275	-0,09	-0,034	-0,204	0,136
22:00	1175	-0,08	-0,020	-0,190	0,150		22:00	1200	-0,06	0,012	-0,158	0,182
23:00	1200	0,02	-0,014	-0,184	0,156		23:00	1300	0,08	0,016	-0,154	0,186



Şekil A.9 : RoC Analiz Sonucu

ÖZGEÇMİŞ

Ad-Soyad **:** Akın ASLAN

Doğum Tarihi ve Yeri **:** 01.07.1981 – İstanbul

E-posta **:** aslan15@itu.edu.tr

ÖĞRENİM DURUMU:

- **Lisans** **:** 2003, Kara Harp Okulu, Elektrik - Elektronik

YAYINLAR, SUNUMLAR VE PATENTLER:

- **Aydın Y., Aslan A.**, 2016: Prevention Against Application Layer 7 DDOS Attacks. 9th International Cyber Security and Cryptography Conference Poster Publication, October 25-26, 2016 Ankara, Turkey.