T.C.
İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

İNTERNET PROTOKOLÜ ÜZERİNDEN SES İLETİŞİMİ İÇİN GÜVENLİK SİSTEMİ TASARIMI VE DEĞERLENDİRİLMESİ: MAKİNE ÖĞRENME TABANLI YAKLAŞIM

Sabit ÇAKIR

DANIŞMAN
Prof. Dr. Ahmet SERTBAŞ

II. DANIŞMAN
Dr. Öğr. Üyesi Muhammed Ali AYDIN

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

İSTANBUL-2019

Bu çalışma 14.10.2019 Tarihinde aşağıdaki jüri tarafından Bilgisayar Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı Yüksek Lisans Tezi olarak kabul edilmiştir.

TEZ JÜRİSİ

Prof. Dr. Ahmet SERTBAŞ
İstanbul Üniversitesi-Cerrahpaşa
Mühendislik Fakültesi

Doç. Dr. Derya YILTAŞ KAPLAN
İstanbul Üniversitesi-Cerrahpaşa
Mühendislik Fakültesi

Doç. Dr. Yusuf YASLAN
İstanbul Teknik Üniversitesi
Bilgisayar ve Bilişim Fakültesi

20.04.2016 tarihli Resmî Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi-Cerrahpaşa'nın abonesi olduğu intihal yazılım programı kullanılarak Lisansüstü Eğitim Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

ÖNSÖZ

Tez çalışması sürecimde desteklerini sürekli yanımda hissettiğim değerli hocalarım Prof. Dr. Ahmet SERTBAŞ ve Dr. Öğr. Üyesi Muhammed Ali AYDIN'a, yine bu süreçte sabır ve anlayışlarıyla yanımda olan tüm dost ve yakınlarıma en içten teşekkürlerimi sunarım.

Ekim 2019 Sabit ÇAKIR

İÇİNDEKİLER

Sayfa No

ÖNSÖZ ..... **iv**
İÇİNDEKİLER ..... **v**
ŞEKİL LİSTESİ ..... **vii**
TABLO LİSTESİ ..... **ix**
SİMGE VE KISALTMA LİSTESİ ..... **x**
ÖZET ..... **xii**
SUMMARY ..... **xiii**
1. GİRİŞ **1**
2. GENEL KISIMLAR **3**
2.1 VOIP SİSTEMLERİ 3
2.1.1 Tarihçe 3
2.1.2 SIP Protokolü Çalışma Prensipleri 4
2.1.3 Bileşenler 5
2.1.4 SIP Mesaj Süreci 6
2.1.5 Diğer İlgili Protokoller 10
2.2 TEHDİT TÜRLERİ 13
2.2.1 Sosyal Tehditler 13
2.2.2 Kulak Hırsızlığı 13
2.2.3 Araya Girme – Değiştirme 15
2.2.4 Hizmet İstismarı 15
2.2.5 Kasıtlı Hizmet Engelleme 16
2.2.6 Fiziksel İhlal 17
2.2.7 Diğer Tehditler 17
2.3 İLGİLİ ÇALIŞMALAR 18
2.4 KULLANILAN ALGORİTMALAR 19
2.4.1 MLP 19
2.4.2 NB (Naive Bayes – Naif Bayes) 25
3. MALZEME VE YÖNTEM **27**
3.1 SİMULASYON 27
3.1.1 BOUN-SIM 27

3.1.2 Trixbox 28
3.1.3 Weka 30
3.2 GELİŞTİRİLEN UYGULAMA 30
4. BULGULAR 35
5. TARTIŞMA VE SONUÇ 53
KAYNAKLAR 54
ÖZGEÇMİŞ 58

ŞEKİL LİSTESİ

Sayfa No

Şekil 2.1: VoIP süreçlerine ait protokollerin konumları. 4

Şekil 2.2: VoIP çağrı sürecinde MGC ve MG ilişkisi [6]. 6

Şekil 2.3: PS üzerinden temel çağrı akışı [8]. 9

Şekil 2.4: SIP INVITE mesajına ait temel başlıklar. 10

Şekil 2.5: SIP INVITE mesajı içeriğindeki SDP mesajı. 12

Şekil 2.6: Temel MLP ağ yapısı. 20

Şekil 3.1: Benzetim şeması. 28

Şekil 3.2: Uygulama benzetim mimarisi. 31

Şekil 3.3: Uygulamaya ait anlık mesaj yoğunluğu görüntüsü. 32

Şekil 3.4: Uygulamaya ait parametre izleme grafikleri. 33

Şekil 3.5: Uygulamaya ait alarm takip ekranı. 34

Şekil 4.1: Sadece arka plan trafiğine ait ısı haritası. 35

Şekil 4.2: 5 x INVITE mesajı ile ısı haritası. 36

Şekil 4.3: 10 x INVITE mesajı ile ısı haritası. 37

Şekil 4.4: 20 x INVITE mesajı ile ısı haritası. 38

Şekil 4.5: 50 x INVITE mesajı ile ısı haritası. 39

Şekil 4.6: 100 x INVITE mesajı ile ısı haritası. 40

Şekil 4.7: 500 x INVITE mesajı ile ısı haritası. 41

Şekil 4.8: 5 x REGISTER mesajı ile ısı haritası. 42

Şekil 4.9: 10 x REGISTER mesajı ile ısı haritası. 43

Şekil 4.10: 20 x REGISTER mesajı ile ısı haritası. 44

Şekil 4.11: 50 x REGISTER mesajı ile ısı haritası. 45

Şekil 4.12: 100 x REGISTER mesajı ile ısı haritası. 46

Şekil 4.13: 500 x REGISTER mesajı ile ısı haritası. 47

Şekil 4.14: Farklı INVITE saldırı yüklerine göre algoritmaların doğruluk cinsinden sınıflandırma başarı düzeyleri. 49

Şekil 4.15: Farklı INVITE saldırı yüklerine göre algoritmaların f skoru cinsinden sınıflandırma başarı düzeyleri. 50

Şekil 4.16: Farklı REGISTER saldırı yüklerine göre algoritmaların doğruluk cinsinden sınıflandırma başarı düzeyleri. 51

Şekil 4.17: Farklı REGISTER saldırı yüklerine göre algoritmaların f skoru cinsinden sınıflandırma başarı düzeyleri. 52

TABLO LİSTESİ

Sayfa No

Tablo 3.1: INVITE sel saldırılarında üretilen yaklaşık anlık paket yükü. 29

Tablo 3.2: REGISTER sel saldırılarında üretilen yaklaşık anlık paket yükü. 29

Tablo 4.1: 5 INVITE paketi yük yoğunluğuna bağlı başarı değerleri. 36

Tablo 4.2: 10 INVITE paketi yük yoğunluğuna bağlı başarı değerleri. 37

Tablo 4.3: 20 INVITE paketi yük yoğunluğuna bağlı başarı değerleri. 38

Tablo 4.4: 50 INVITE paketi yük yoğunluğuna bağlı başarı değerleri. 39

Tablo 4.5: 100 INVITE paketi yük yoğunluğuna bağlı başarı değerleri. 40

Tablo 4.6: 500 INVITE paketi yük yoğunluğuna bağlı başarı değerleri. 41

Tablo 4.7: 5 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri. 42

Tablo 4.8: 10 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri. 43

Tablo 4.9: 20 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri. 44

Tablo 4.10: 50 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri. 45

Tablo 4.11: 100 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri. 46

Tablo 4.12: 500 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri. 47

SİMGE VE KISALTMA LİSTESİ

Simgeler	Açıklama
$Ç_i$	: Yapay sinir ağına ait i numaralı çıkış
$\boldsymbol{\beta}$	: Yapay sinir ağı eşik değeri
$\boldsymbol{\delta_m}$	: m. numaralı sinir hücresine ait hata
$\boldsymbol{A}$	: Yapay sinir hücresine ait girdi ağırlığı

Kısaltmalar	Açıklama
CSV	: Comma Separated Values – Virgülle Ayrılmış Değerler
DDoS	: Distributed Denial of Service – Dağıtık Hizmet Engelleme
DoS	: Denial of Service – Hizmet Engelleme
HTTP	: Hyper Text Transfer Protocol – Hiper Metin Aktarım Protokolü
IDS	: Intrusion Detection System – İhlal Denetleme Sistemi
IETF	: Internet Engineering Task Force – İnternet Mühendisliği Görev Gücü
IP	: Internet Protocol – İnternet Protokolü
IPDC	: Internet Protocol Device Control – İnternet Protokolü Cihaz Denetimi
IPS	: Intrusion Prevention System – İhlal Engelleme Sistemi
ITU	: International Telecommunication Union – Uluslararası Telekomunikasyon Birliği
JSON	: JavaScript Object Notation – JavaScript Nesne Gösterimi
MAP	: Maximum A Posteriori – En Büyük Sonrasal
MDCP	: Media Device Control Protocol – Veri Cihazı Kontrol Protokolü
MG	: Media Gateway – Veri Ağ Geçidi
MGC	: Media Gateway Controller – Veri Ağ Geçidi Kontrol Birimi
MGCP	: Media Gateway Control Protocol – Veri Ağ Geçidi Kontrol Protokolü
MLP	: Multi Layer Perceptron – Çok Katmanlı Algılayıcı
PS	: Proxy Server – Vekil Sunucu
PSTN	: Public Switched Telephone Network – Genel Aktarmalı Telefon Şebekesi
QoS	: Quality of Service – Hizmet Kalitesi
RAM	: Random Access Memory – Rastgele Erişimli Bellek
REST	: Representational State Transfer – Temsili Durum Aktarımı

RNN : Random Neural Network – Rastgele Sinir Ağı

RTCP : Real Time Transport Control Protocol – Gerçek Zamanlı İletim Kontrol Protokolü

RTP : Real Time Transport Protocol – Gerçek Zamanlı İletim Protokolü

SCIP : Simple Conference Invitation Protocol – Basit Konferans Davet Protokolü

SDP : Session Description Protocol – Oturum Tanımlama Protokolü

SGCP : Simple Gateway Control Protocol – Basit Ağ Geçidi Kontrol Protokolü

SIP : Session Initiation Protocol – Oturum Başlatma Protokolü

SIP URI : Session Initiation Protocol Uniform Resource Identifier – Oturum Başlatma Protokolü Tekdüzen Kaynak Tanımlayıcı

SVM : Support Vector Machine – Destek Vektör Makinesi

SVR : Support Vector Regression – Destek Vektör Regresyonu

TCP/IP : Transmission Control Protocol/Internet Protocol – İletim Kontrol Protokolü/İnternet Protokolü

UA : User Agent – Kullanıcı Etmeni

UAC : User Agent Client – Kullanıcı Etmeni İstemci

UAS : User Agent Server – Kullanıcı Etmeni Sunucu

VMON : Voice Over Internet Protocol Monitoring – İnternet Protokolü Üzerinden Ses İletimi İzleme

VoIP : Voice Over Internet Protocol – İnternet Protokolü Üzerinden Ses İletişimi

ÖZET

YÜKSEK LİSANS TEZİ

İNTERNET PROTOKOLÜ ÜZERİNDEN SES İLETİŞİMİ İÇİN GÜVENLİK SİSTEMİ TASARIMI VE DEĞERLENDİRİLMESİ: MAKİNE ÖĞRENME TABANLI YAKLAŞIM

Sabit ÇAKIR

İstanbul Üniversitesi-Cerrahpaşa

Lisansüstü Eğitim Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman : Prof. Dr. Ahmet SERTBAŞ

II. Danışman : Dr. Öğr. Üyesi Muhammed Ali AYDIN

Günümüzde IP (Internet Protocol – İnternet Protokolü) tabanlı sistemlerin gelişmesiyle birlikte paket anahtarlamalı ağlar devre anahtarlamalı ağların yerini almaya başlamış ve maliyet avantajları sebebiyle operatörler arasında daha fazla tercih edilir olmuştur. Bununla birlikte VoIP (Voice Over Internet Protocol – İnternet Protokolü Üzerinden Ses İletişimi) sistemleri, IP tabanlı sistemlerin açık olduğu tehditlere aynı şekilde açık olması sebebiyle farklı güvenlik ve izleme mekanizmaları önerilmiştir. Benzer şekilde, bu tez çalışmasında da bir VoIP güvenlik sistemi tasarımı önerilmiştir. Geliştirme sürecinde PS (Proxy Server – Vekil Sunucu) üzerinde sağlıklı SIP (Session Initiation Protocol – Oturum Başlatma Protokolü) trafik benzetimi ve DoS (Denial of Service – Hizmet Engelleme) saldırısı içeren trafik benzetimi gerçekleştirilmiş, PS üzerinden geçen SIP mesaj yük yoğunlukları makine öğrenme teknikleri ile test edilmiş, sağlıklı ve DoS saldırısı içeren trafiğin sınıflandırılma başarı düzeyleri incelenmiştir. Değerlendirme sonucunda trafiği SIP mesaj histogramlarını kullanarak sınıflandıran MLP (Çok Katmanlı Algılayıcı – Multi Layer Perceptron) tabanlı bir uygulama prototipi geliştirilmiştir.

Ekim 2019, 71 sayfa.

Anahtar kelimeler: VoIP, SIP, Siber Güvenlik, İhlal Denetleme Sistemi, Makine Öğrenmesi

SUMMARY

M.Sc. THESIS

SECURITY SYSTEM DESIGN AND EVALUATIONS FOR VOIP COMMUNICATION: MACHINE LEARNING BASED APPROACH

Sabit ÇAKIR

Istanbul University-Cerrahpasa

Institute of Graduate Studies

Department of Computer Engineering

Supervisor : Prof. Dr. Ahmet SERTBAŞ

Co-Supervisor : Dr. Muhammed Ali AYDIN

Novadays, with the advancement of IP (Internet Protocol) based systems, packet switched networks started substutioning with circuit switched networks in telecommunication systems and become more preferable among operators due to their cost advantages. In addition, different security and monitoring mechanisms have been suggested as VoIP (Voice Over Internet Protocol) systems are equally vulnerable to threats such as IP based systems have. Similarly, in this thesis, a VoIP security system design is proposed. Healthy SIP (Session Initiation Protocol) traffic and DoS (Denial of Service) attack traffic simulations are performed on PS (Proxy Server), SIP message load densities on PS are tested via machine learning methods and success levels of traffic classication as healthy and DoS attack are evaluated during the development process. At the result of the evaluation, a MLP (Multi Layer Perceptron) based program prototype is developed which classifies SIP traffic by using SIP message histograms.

October 2019, 71 pages.

Keywords: VoIP, SIP, Cyber Security, Intrusion Detection System, Machine Learning

1. GİRİŞ

Günümüzde teknolojinin tüm alanlarındaki gelişmelere paralel olarak iletişim sistemlerindeki gelişme de büyük bir hızla devam etmektedir. İnternet teknolojilerindeki gelişmeler sonucunda iletişim sistemlerinde PSTN (Public Switched Telephone Network – Genel Aktarmalı Telefon Şebekesi) tabanlı iletişim altyapısının yerini verim ve maliyet avantajları sebebiyle IP tabanlı sistemler almaya başlamıştır. IP tabanlı sistemlerin kullanımının artmasıyla birlikte VoIP iletişim sistemleri ve VoIP oturumunun organize edilmesini sağlayan SIP protokolü oldukça geniş bir alanda kullanılmaya başlanmıştır. 2014 yılında, VoIP hizmetlerine ait pazarın 2020 yılı itibariyle 348.5 milyon kullanıcı ile 136.76 milyar dolarlık bir bütçeye ulaşması beklendiği raporlanmıştır [1]. Bu sistemlerin kullanım alanındaki kaynak verimliliği gibi avantajlarıyla birlikte internet teknolojilerinin açık olduğu tehditlere açık olması, bu teknolojinin daha yakından takip edilmesi zorunluluğunu doğurmuştur.

Operatörler açısından yaklaşıldığında müşteri güveninin devamı, QoS (Quality of Service – Hizmet Kalitesi) kavramı ve hizmet sürekliliğinin sağlanmasıyla doğrudan alakalıdır lakin mevcut tedbirlere rağmen operatörler her yıl internet üzerindeki dolandırıcılık ve DoS saldırıları gibi tehditler sebebiyle oldukça büyük bir bütçe kaybına uğramaktadırlar. Geleneksel iletişim ağlarındaki dolandırıcılık sebebiyle operatörlerin 2010 yılı itibariyle her yıl %3 ila %5 kazanç kaybettikleri ve bu tehdidin mevcut süreçte %10 üzerinde artışla devam ettiği raporlanmış, ayrıca güçlü güvenlik sistemlerinin eksikliği gibi sebeplerle VoIP ağlarında bu tehditin daha olumsuz sonuçlara yol açması beklendiği ifade edilmiştir [2]. Bahsedilen tehditlerin bertaraf edilmesi maksadıyla firmalar ve araştırmacılar farklı güvenlik çözümleri üzerinde çalışmaktadırlar. Bu çözümler IDS (Intrusion Detection System – İhlal Denetleme Sistemi), IPS (Intrusion Prevention System – İhlal Engelleme Sistemi), kara liste (black list), beyaz liste (white list), politika yöneticisi (policy manager) ve VMON (Voice Over Internet Protocol Monitoring – İnternet Protokolü Üzerinden Ses İletimi İzleme) sistemleri gibi çözümlerdir. Klasik sistemler kural tabanlı yöntemlerle çözüm sağlamaya çalışırken, tehdit kaynaklarının her geçen gün artması sebebiyle teknolojideki akıllı sistemlere yönelim burada da karşılık bulmuş ve bu tehditlere karşı sezgisel ya da makine öğrenmesi tabanlı sistemlerin kullanım verimi araştırmacılar tarafından değerlendirilmiştir.

Bu tez çalışmasında da benzer şekilde VoIP ağlarındaki mevcut tehditlerden biri olan DoS saldırısının belirlenebilmesi amacıyla bir yöntem olarak makine öğrenmesinin başarı düzeyinin değerlendirilmesi amaçlanmış ve temel bir makine öğrenme tabanlı VoIP izleme sistemi prototipi geliştirilmiştir.

Bu tezin 1.bölümünde tez hakkında kısa bilgi verilmiş ve amacı açıklanmış, 2. bölümünde ilgili teknolojik altyapı hakkında genel bilgi verilerek literatür özeti anlatılmış, 3. bölümünde benzetim ortamı bileşenleri ve geliştirilen uygulama hakkında bilgi verilmiş, 4. bölümünde benzetim sonuçları belirtilerek değerlendirmeler yapılmış ve son olarak 5. bölümde çalışmaya ait nihai sonuç ifade edilerek daha sonraki çalışmalar için değerlendirmeler anlatılmıştır.

2. GENEL KISIMLAR

2.1 VOIP SİSTEMLERİ

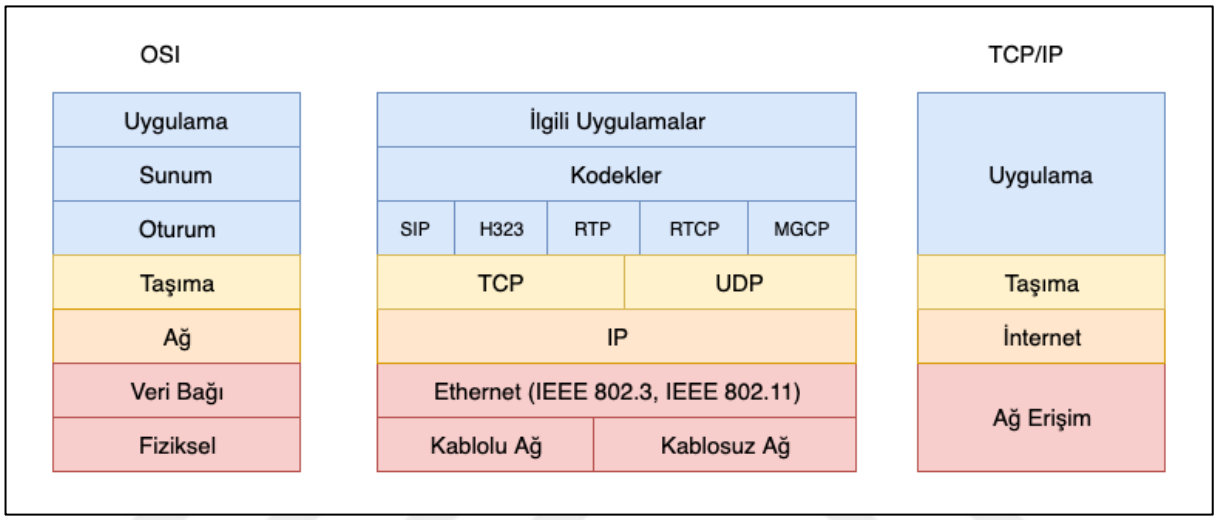
2.1.1 Tarihçe

VoIP sistemleri internetin gelişmesiyle birlikte ağ verimi ile birlikte çoklu ortam konferans, görüntülü veri iletimi, anlık mesajlaşma gibi yetenekleri sebebiyle PSTN ağların hızla yerini almaya başlamıştır. Günümüz IP çoklu ortam iletişim sistemleri aslında içeriğinde birden fazla protokolü barındırmaktadır. VoIP sistemlerinde ise uygulama katmanında H.323 ve SIP protokolü kullanılmaktadır. Bu iki protokol çıkış yılı itibariyle ikisi de 1996 yılında kabul edilen protokollerdir. Bugün ise SIP protokolü VoIP sistemlerin standardı haline gelmiştir. Öncelikle 1996 yılında Handley ve Schooler tarafından SIP (Session Invitation Protocol – Oturum Davet Protokolü) -bugün kullandığımız Oturum Başlatma Protokolünden farklı fakat aynı kısaltma ile ifade ediliyor- ve Schulzrinne tarafından SCIP (Simple Conference Invitation Protocol – Basit Konferans Davet Protokolü) taslak formları oluşturulmuştur. Bu çalışmalarda ilk etapta amaç internet çoklu ortamı için birden çok kişiyi konferans yayınlarına davet etmekti. Bu amaçla yazılan ilk taslaklar “draft-ietf-mmusic-scip-00” ve “draft-ietf-mmusic-sip-00” isimleriyle bilinmektedirler. İlk yapıda çağrı kurulumunu sağlayan tek bir Talep (Request) mesaj tipi mevcuttu. Daha sonra Aralık 1996’da “draft-ietf-mmusic-sip-01” ve Ocak 1999’da “draft-ietf-mmusic-sip-12” taslakları oluşturuldu. Bu son taslakta bugün SIP protokolünde kullanılan altı SIP talep tipi mevcuttu. Mart 1999’da ise bugünkü SIP standartlarının temeli olan RFC 2543 standartları yayınlandı [3]. Son olarak 2002 yılında RFC 3261 standartları yayınlanmıştır [4].

Günümüzde SIP protokolü VoIP iletişiminin standart protokolü haline gelmiştir. SIP protokolü aracılığıyla kullanıcı konumlarının belirlenmesi, kullanılacak çoklu ortam içeriklerinin parametrelerinin belirlenmesi, kullanıcıların oturuma katılım imkanlarının belirlenmesi, çağrı kurulum ve yönetim süreçleri şekillendirilebilmektedir. İki uçbirim arasında oturum tanımı bilgisi SDP (Oturum Tanımlama Protokolü – Session Description Protocol) aracılığıyla, çoklu ortam verilerinin transferi ise RTP (Gerçek Zamanlı İletim Protokolü – Real Time Transport Protocol) vasıtasıyla yapılmaktadır.

2.1.2 SIP Protokolü Çalışma Prensipleri

SIP protokolü TCP/IP (Transmission Control Protocol/Internet Protocol – İletim Kontrol Protokolü/İnternet Protokolü) modelinde uygulama katmanında yer almaktadır. OSI (Open System Interconnection – Açık Sistem Arabağlantısı) sisteminde ise Oturum (Session) katmanında yer almaktadır. SIP protokolü ve bağlantılı bazı protokollerin ilgili ağ modellerindeki konumu Şekil 2.1'de gösterilmiştir.



Şekil 2.1: VoIP süreçlerine ait protokollerin konumları.

SIP protokolünün davranışı HTTP (Hyper-Text Transfer Protocol – Hiper Metin Aktarım Protokolü) protokolünün davranışına oldukça benzemektedir. TCP/IP modelinde bir uygulama katmanı protokolü olan SIP'te her bir kullanıcı adresi SIP URI (Session Initiation Protocol Uniform Resource Identifier – Oturum Başlatma Protokolü Tekdüzen Kaynak Tanımlayıcı) ile tanımlanır. SIP URI yapı olarak e-posta adresine oldukça benzemektedir. Örnek bir SIP URI formu kullanici@domain.com şeklinde ifade edilebilir. Bu adres kullanıcının bağlı olduğu domaine ait PS tarafından çözümlenir. Kullanıcının IP adresi olarak gerçek konumunun tanımlanabilmesi için ayrıca kullanıcının konumu, daha önce ilgili domaine ait konum sunucusu (Location Server) tarafında kayıtlı olmalıdır. Kullanıcı başka bir kullanıcıyı oturum için davet ettiğinde kullanıcının ait olduğu domaine ait PS yine ilgili domaine ait konum sunucusu tarafından aranan kullanıcının IP adresi olarak gerçek konumunu edinmeye çalışır [2]. Bu şekilde aranan kullanıcıya ulaşılır ve aranan kullanıcı dilediği taktirde oturum

başlatmayı onaylar veya reddeder. Gelen mesaj onaylanırsa RTP protokolü üzerinden çoklu ortam yayını başlar.

2.1.3 Bileşenler

SIP trafiğinin kullanıldığı sistemler aşağıdaki birimlerden oluşmaktadır.

UA (User Agent – Kullanıcı Etmeni): İki tarafın iletişim için kullandığı fiziksel telefon ya da bilgisayar yazılımıdır [5]. UA mesajlaşmadaki konumuna göre aşağıdaki gibi iki şekilde ifade edilebilir.

UAC (User Agent Client – Kullanıcı Etmeni İstemci): SIP sinyalleşmesini başlatan istemcidir [5]. Bu birim, fiziksel bir telefon olabileceği gibi bir bilgisayar yazılımı da olabilir.

UAS (User Agent Server – Kullanıcı Etmeni Sunucu): İstemciden gelen SIP mesajlarına cevap veren sunucudur [5]. Bu birim, fiziksel bir telefon olabileceği gibi bir bilgisayar yazılımı da olabilir.

PS: Farklı İki UA arasında iletişim başlatılması için SIP trafiğinin organize edildiği birimdir. PS farklı konumdaki bir sunucuya SIP mesajı göndermek için hem sunucu, hem de istemci olarak davranır [5].

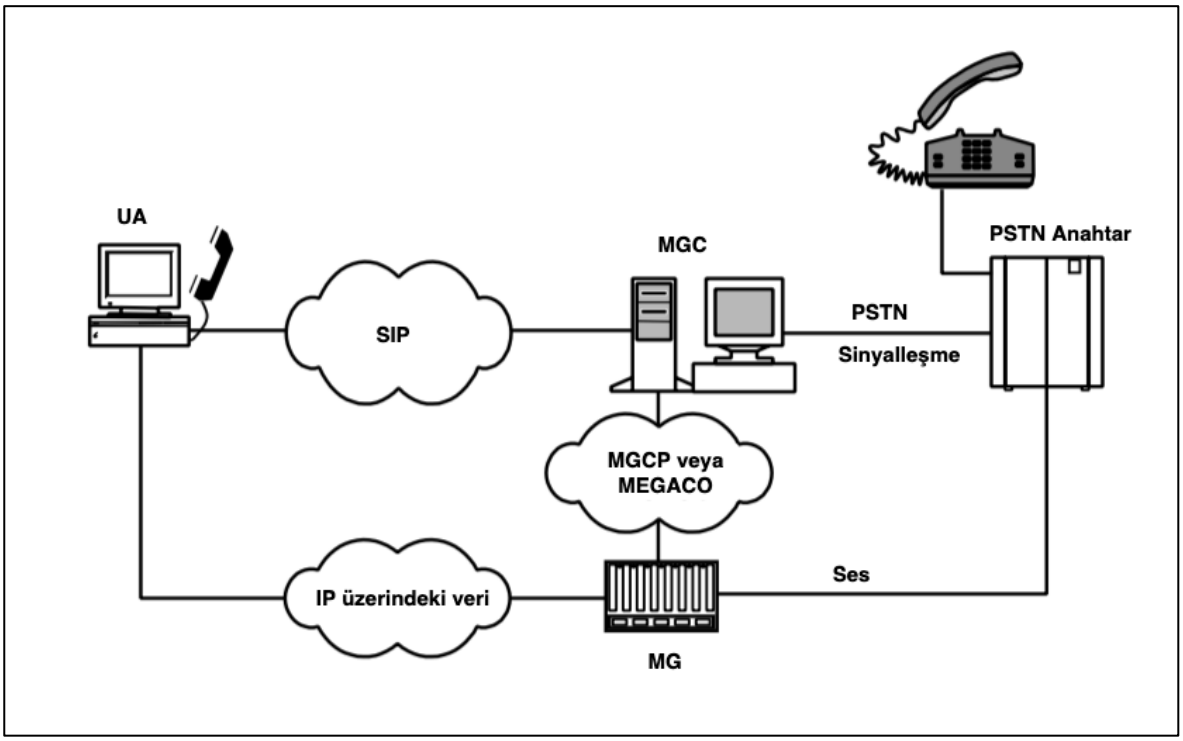
Yönlendirme Sunucusu (Redirect Server): Gelen SIP talebine cevap olarak aranan birim yerine ihtiyaç durumunda alternatif adres sağlayan birimdir.

Kayıt Sunucusu (Registrar Server): Gelen SIP REGISTER talep mesajını kabul edip, mesajla birlikte gelen bilgiyi ilgili domaine ait konum sunucusuna kaydeden sunucudur [5].

Konum Sunucusu: Kullanıcıların iletişim adresleri ve konum bilgilerini muhafaza edip, PS ve kayıt sunucularına bu bilgiyi sağlayan sunucudur [5].

MG (Media Gateway – Veri Ağ Geçidi): Günümüz iletişim sistemlerinde PSTN ağlar ve IP ağları arasında sorunsuz bir etkileşim mevcuttur. VoIP ağlarından yapılan çağrılarda verinin PSTN ağlarındaki dönüşümünü yapan birim MG'dir. Genelde tercih edilen mimari, SIP sinyalleşmesinin yönetildiği MGC (Media Gateway Controller – Veri Ağ Geçidi Kontrol Birimi) ve MG arasında iletişimin sağlandığı mantıksal bir dizayndır. Bu mimaride MGC, PS görevi görmekte ve sinyalleşme bu birim üzerinden yönetilmektedir [6]. Veri yönetimi ise MG

tarafından organize edilirken iki birim arasındaki yönetimsel iletişim MGCP (Media Gateway Control Protocol – Veri Ağ Geçidi Kontrol Protokolü) veya Megaco -Megaco aynı zamanda MGCP gibi Veri Ağ Geçidi Kontrol Protokolü anlamına gelmektedir fakat farklı bir protokoldür- ismi verilen özel protokoller aracılığıyla sağlanmaktadır. İlgili mimariye ait grafik Şekil 2.2'de gösterilmiştir. İlgili protokollerle alakalı bilgi bölüm 2.1.5'te verilmiştir.



Şekil 2.2: VoIP çağrı sürecinde MGC ve MG ilişkisi [6].

2.1.4 SIP Mesaj Süreci

SIP Transaction (SIP İşlem): SIP Mesaj yapısı ile alakalı bilgiler RFC 3261'de detaylı bir şekilde ifade edilmiştir. SIP Mesajlarında her bir talebe karşılık, o mesaja bağlı olarak verilen son cevaba (response) kadar süreci içeren mesajlaşmaya SIP Transaction denir [5].

SIP Dialog (SIP Diyalog): Bir başarılı SIP oturum başlangıcından oturum bitirilene kadar olan tüm SIP mesajlaşma süreci SIP Dialog şeklinde adlandırılmaktadır [5].

SIP mesajları Talep (Request) ve Cevap (Response) mesajları olmak üzere ikiye ayrılmaktadır.

Temel 6 Talep mesajı aşağıda ifade edilmiştir.

- INVITE**:** Kullanıcı talebiyle bir SIP oturumunu başlatmak amacıyla kullanılır.
- BYE**:** Çağrıyı sonlandırılması amacıyla kullanılan mesajdır.
- REGISTER**:** Kullanıcının bir kayıt sunucusuna bilgileriyle kayıt olması amacıyla kullanılır.
- CANCEL**:** Başlamış bir çağrı talebine karşılık henüz başlamamış bir oturumun sonlandırılması amacıyla kullanılır.
- ACK**:** INVITE mesajıyla başlanan oturum talebi ACK mesajıyla tanımlanmış olur. ACK mesajıyla birlikte SDP mesaj yükü de gönderilir ve daha sonra RTP veri aktarımı başlar.
- OPTIONS**:** PS tarafından, UA ya da PS'lerin erişilebilirlik durumunu kontrol etmek amacıyla kullanılır.

Ayrıca daha özel durumlarda kullanılan SUBSCRIBE, NOTIFY, PUBLISH, REFER, INFO, UPDATE, PRACK ve MESSAGE gibi SIP mesajları da ifade edilebilir.

SIP cevap mesajları ise altı grupta ifade edilebilir. En sık kullanılan bazı SIP cevap mesajları aşağıda gösterilmiştir.

- 1xx: Bilgi Mesajları
    - 100 Trying: Ulaşılmaya çalışılıyor
    - 180 Ringing: Karşı tarafta telefon çalıyor
    - 181 Call is Being Forwarded: Çağrı yönlendiriliyor
    - 182 Call Queued: Çağrı kuyruğa alındı
    - 183 Session Progress: Oturum işleniyor

- 2xx: Başarı Mesajları
    - 200 OK: Başarılı cevabı
    - 202 Accepted: Kabul cevabı

- 3xx: Yönlendirme Mesajları
    - 301 Moved Permanently: Kalıcı olarak konum değişti
    - 302 Moved Temporarily: Geçici olarak konum değişti

- 4xx: İstemci Başarısızlık mesajları
    - 400 Bad Request: Hatalı talep içeriği
    - 401 Unauthorized: Yetki mevcut değil
    - 403 Forbidden: Yasaklanmış
    - 404 Not Found: Hedef bulunamadı
    - 405 Method Not Allowed: Yöntem kabul edilmiyor

- 5xx: Sunucu Başarısızlık Mesajları
    - 500 Server Internal Error: Dahili sunucu hatası
    - 501 Not Implemented: İlgili mesaja ait uygulama mevcut değil
    - 502 Bad Request: Hatalı talep
    - 503 Service Unavailable: Hizmet şu an mevcut değil

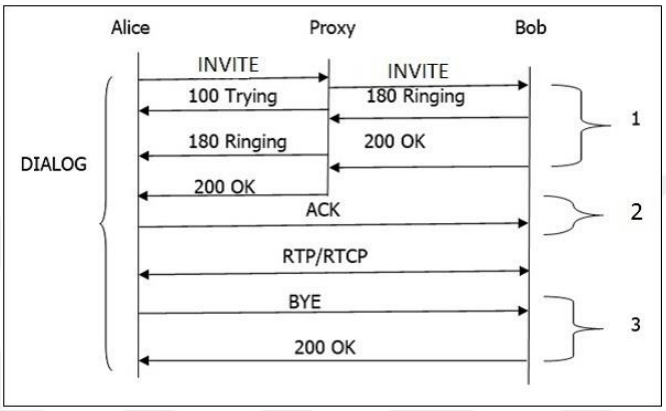
- 6xx: Genel Başarısızlık Mesajları
    - 600 Busy Everywhere: Tüm hedefler meşgul
    - 603 Decline: Çağrı reddedildi
    - 606 Not Acceptable: Çağrı kabul edilemiyor

[7]

Temel SIP mesajlaşması Şekil 2.3'de görselleştirilmiştir. Bu görseldeki SIP oturumunda sırasıyla aşağıda ifade edilen işlemler gerçekleşmektedir.

- Öncelikle kullanıcı Alice oturum başlatma isteğini Bob'a bildirmek için bağlı olduğu SIP PS'ye iletir.
- Bu arada ilgili PS hemen Alice'ten yeniden gereksiz INVITE mesajı almamak için Alice'e Bob'a erişmeye çalıştığını ifade eden 100 Trying mesajı gönderir.
- Sonra PS ilgili konum sunucusundan Bob'un adres bilgisini ister ve bu bilgiyi aldıktan sonra Alice'ten gelen INVITE mesajını Bob'a yönlendirir.
- Daha sonra Bob tarafında telefonun çaldığı bilgisini ifade eden 180 Ringing üretilir ve PS aracılığıyla yine Alice'e iletilir.
- Sonrasında Bob telefon ahizesini kaldırdığında SIP oturumunu onaylamış olur ve PS vasıtasıyla 200 OK mesajı Alice tarafına iletilir.

- Alice 200 OK mesajını aldığında Bob'ta ACK mesajını alır.
- ACK mesajından sonra SIP oturumu başlamış olur ve doğrudan iki uç arasında RTP çoklu ortam akışı başlar.
- Konuşma bittikten sonra iki taraftan biri oturumu sonlandırmak istediğinde karşı tarafa doğrudan BYE mesajı gönderir.
- Diğer taraf doğrudan 200 OK mesajı gönderir ve oturum bu şekilde sonlanmış olur [8].



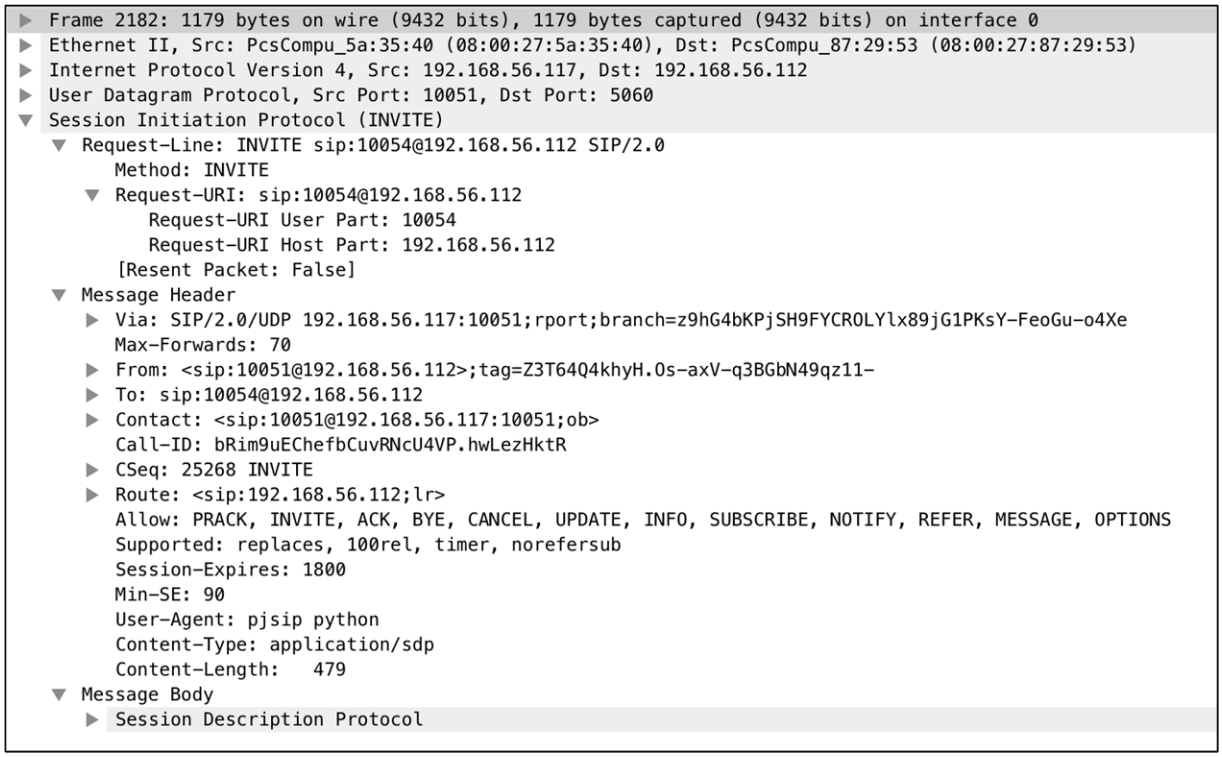
Şekil 2.3: PS üzerinden temel çağrı akışı [8].

Wireshark uygulaması aracılığıyla yakalanan bir SIP INVITE mesajına ait örnek içerik Şekil 2.4'te gösterilmiştir.

Buradaki başlıkların kullanım amaçları aşağıdaki gibidir.

- Request-Line: İlgili SIP mesajının gideceği hedef ile birlikte kullanılan SIP protokol versiyonunu ifade etmektedir.
- Via: SIP protokol versiyonu, taşıma katmanı protokolü, IP adres ve port bilgileri taşır. Bu bilgilerle mesajın doğru cihaza gitmesi sağlanır.
- From: Mesaj kaynağını ifade eder.
- To: Mesaj hedefini ifade eder.
- Contact: Aranan daha sonraki taleplerde, çağrı kaynağına erişmek için bu başlık kullanılır.
- Call-ID: Bir SIP oturumuna ait tüm mesajlaşmanın o oturuma ait olduğunu ifade eden benzersiz bir kimlik bilgisidir.

- CSeq: Kullanıcı etmeni tarafından oturum bitene kadar gönderilen (her bir talep mesajıyla artan) sıra numarası ve mesaj tipinden oluşan ifadedir .
- Route: PS mesajlaşmanın kaynak ve hedef arasında doğrudan değil, kendi üzerinden geçmesini istediğinde bu başlık kullanılır [4].



Şekil 2.4: SIP INVITE mesajına ait temel başlıklar.

2.1.5 Diğer İlgili Protokoller

RTP Protokolü

RTP Protokolü, SIP oturumuna bağlı ses ve görüntü verisinin aktarımında kullanılmaktadır. RTP protokolü standartları RFC 3550 ile belirlenmiştir. RTP protokolü, taşıma katmanında UDP kullanmaktadır. RTP protokolünde veriler taşınmak için kodek (codec) yazılımı vasıtasıyla paketlenir. RTP protokolü, temel olarak gelen ve giden paketlerin içerik gereksinimlerinin ve zamanlanmasının belirlenmesi için aşağıdaki bilgileri kullanır.

- Sıra numarası (Sequence number)
- Yeniden iletim olmadan paket yönlendirme (Packet forward without retransmission)

- Kaynak tanımlama (Source identification)
- İçerik tanımlama (Content identification)
- Eşzamanlılık (Syncronism)

RTP protokolü veri iletimine ait değerlerin izlenmesi amacıyla RTCP (Real Time Control Protocol – Gerçek Zamanlı Kontrol Protokolü) ile birlikte çalışmaktadır [5].

RTCP Protokolü

RTCP protokolü, aktarılan verinin kalitesinin izlenmesi için QoS ve VMON süreçlerinde kullanılan temel bir protokoldür. Bu protokol RTP veri iletimine ait sürekli band dışı bir geribildirim kaynağıdır. RTCP vasıtasıyla veri gecikmesi (delay), gecikmedeki değişim (jitter), gidiş dönüş süresi (round trip time) ve paket kaybı (packet loss) değerleri sürekli izlenebilir ve ses kalitesine ait metrikler takip edilebilir [5].

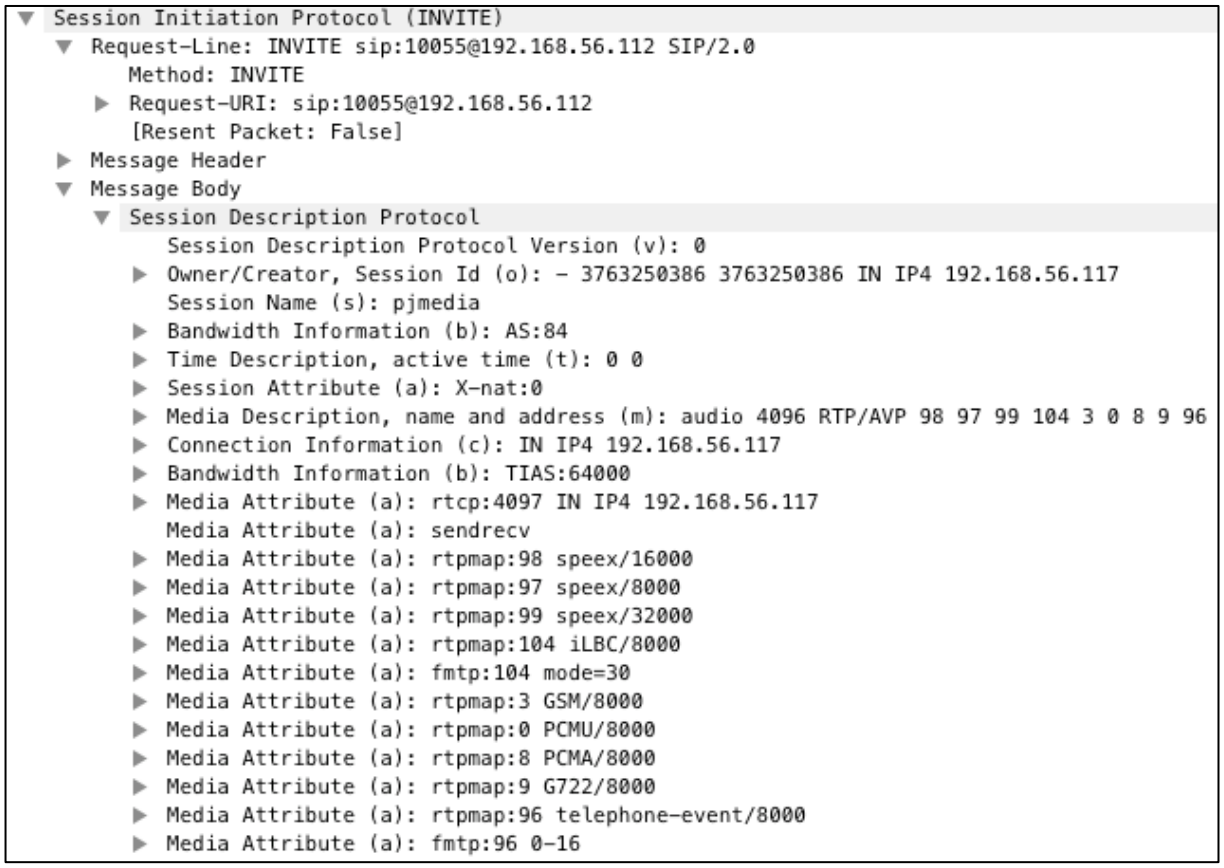
SDP Protokolü

SDP protokolü RFC 4566'da açıklanmıştır. SDP protokolü iki UA arasında oturuma ait parametrelerin transferinde kullanılır. İletişim adresleri, iletilen veriye ait detay bilgileri ve iletilen veriyle alakalı diğer bilgiler SDP protokolü aracılığıyla paylaşılmaktadır. Normal koşullarda SIP INVITE ve 200 OK mesajları yüklerinde (payload) SDP mesajlarını taşımaktadır [5]. Wireshark uygulaması aracılığıyla elde edilen örnek bir SDP mesaj içeriği Şekil 2.5'te gösterilmiştir. SDP paketinde aslında her satır tek bir karakter ile gösterilmektedir. Wireshark uygulaması bu değerlerin ne anlama geldiğini de ayrıca göstermektedir. Burada görüntülenen zorunlu alanlar ve anlamları aşağıdaki gibidir [5].

- **v:** SDP paketine ait protokol versiyonu
- **o:** Oturum kaynağı
- **s:** Oturum adı
- **t:** Oturum başlama ve bitiş zamanı
- **m:** Veri tipi

MGCP (Media Gateway Control Protocol – Veri Ağ Geçidi Kontrol Protokolü)

MGCP protokolü VoIP mekanizmasındaki süreçlere ait ayrık mantıksal bileşenlerin (MG ve MGC) iletişimini sağlamak amacıyla kullanılmaktadır. MGCP çağrı süresince SIP ve H.323 protokollerinin tamamlayıcı protokolüdür.



Şekil 2.5: SIP INVITE mesajı içeriğindeki SDP mesajı.

MGCP protokolü SGCP (Simple Gateway Control Protocol – Basit Ağ Geçidi Kontrol Protokolü) ve IPDC (Internet Protocol Device Control – İnternet Protokolü Cihaz Denetimi) protokollerinin birleştirilmesi sonucunda ortaya çıkmıştır [9]. RFC 2805 "MGCP mimari ve gereksinimleri" dağıtık MG fonksiyonlarını tanımlayan resmi belge konumundadır [6].

Megaco Protokolü

Ayrıca H.248 olarak ta bilinen Megaco protokolü ilk olarak ITU (International Telecommunication Union – Uluslararası Telekomünikasyon Birliği) birliği tarafından Nisan 1999'da kabul edildi. Daha sonra IETF (Internet Engineering Task Force – İnternet

Mühendisliği Görev Gücü) tarafından MGCP ve MDCP (Media Device Control Protocol – Veri Cihazı Kontrol Protokolü) protokollerini uzlaştırmak üzere çalışmalara başlandı. Megaco/H.248 Haziran 1999'da dağıtık ağ geçidi mimarisi için MGC ve MG'ler arasında arayüz niteliği taşıyan protokol standardı olarak ITU ve IETF tarafından tek doküman olarak yayınlandı. Megaco, MGCP'den türetildiği için MGCP ve Megaco arasında birçok benzerlik vardır [9].

2.2 TEHDİT TÜRLERİ

VoIP alanındaki tehditleri sınıflandırmak istediğimizde VoIPSA organizasyonuna ait sınıflandırmadan faydalanabiliriz. VoIPSA farklı satıcı ve bireysel katılımcılardan oluşan; VoIP güvenliği ile ilgilenen, kâr amacı gütmeyen bir organizasyondur [10].

Bu sınıflandırmaya göre tehditler kabaca aşağıdaki gibi ifade edilebilir.

2.2.1 Sosyal Tehditler

Bu kısım daha çok insan hatalarından oluşan kanunsuz ve yetkisiz kullanıma imkân oluşturan durumlara odaklanmaktadır. Aşağıda bu kapsamdaki belirli maddeler ifade edilmiştir.

Yanlış Bilgi: Kasıtlı olarak; yanlış kimlik, yanlış otorite bilgisi, hakların yanlış beyanıyla alakalı tehditler ve yanlış içeriklerden doğan tehditler bu kapsamdadır. Örnek verilecek olursa; bir ağa erişip konfigürasyonu değiştirmek gibi amaçlarla yapılan oltalama (phishing) saldırılarının temel bileşeni yanlış bilgidir.

Hizmet Hırsızlığı: Servis sağlayıcıya ait ödeme kayıtlarının yetkisiz olarak silinmesi, yasal ödeme mekanizmasının yetkisiz olarak çalışmaz hale getirilmesi gibi servis sağlayıcıya ekonomik zarar veren eylemler bu kapsamda değerlendirilmektedir.

İstenmeyen İletişim: Bu kısım, kişilerin onayları olmaksızın gelen çağrılar vasıtasıyla rahatsız edildikleri iletişim şekillerini ifade etmektedir [11].

2.2.2 Kulak Hırsızlığı

Kulak hırsızlığı, saldırganın iki uçbirim arasına girerek aradaki tüm trafiği izleme imkanına ulaştığı saldırı yöntemlerini ifade etmektedir.

Çağrı Deseni İzleme: Bir ağdaki iki uç arasındaki her türlü yetkisiz trafik deseni izleme, kümeleme ve analiz eylemi bu kapsamda değerlendirilebilir. Bu yöntemle kimlik yakalama, herhangi bir bilginin mevcudiyetini belirleme, hırsızlık, gasp ve oltalama saldırısı gibi yetkisiz müdahale eylemlerinin ilk aşaması gerçekleştirilebilir.

Trafik Yakalama: Trafikte akan paketlerin, tarafların onayı alınmadan; yetki dışı amaçlar doğrultusunda loglanması, kaydedilmesi gibi eylemler bu çerçevede değerlendirilebilir.

Sayı Hasadı: Sayı hasadı, kimlik bilgileri gibi verilerin farklı bir yetkiyi kullanarak yetki dışı bir şekilde toplanmasını ifade etmektedir.

Konuşma Yeniden Yapılandırma: Konuşma yeniden yapılandırma, iki birim arasındaki sesli iletişim esnasında tarafların onayı alınmadan; ses bilgisinin toplaması, izlenmesi, yorumlanması, kaydedilmesi ve özellik çıkarılması gibi aktiviteleri ifade etmektedir.

Ses Postası Yeniden Yapılandırma: Ses postası yeniden yapılandırma, iki birim arasındaki ses postası iletişiminin tarafların onayı alınmadan; toplanması, izlenmesi, yorumlanması, kaydedilmesi ve özellik çıkarılması gibi aktiviteleri ifade etmektedir.

Faks Yeniden Yapılandırma: Faks yeniden yapılandırma, iki birim arasındaki iletişimdeki sayısal doküman görseli üzerinden tarafların onayı alınmadan; kimlik bilgisi, durum ve özel bilgi mevcudiyeti gibi verilerin toplanması, izlenmesi, yorumlanması, kaydedilmesi ve özellik çıkarılması gibi aktiviteleri ifade etmektedir.

Video Yeniden Yapılandırma: Video yeniden yapılandırma, iki birim arasındaki iletişimdeki video üzerinden tarafların onayı alınmadan; kimlik bilgisi, durum bilgisi, özel bilgi mevcudiyeti gibi verilerin toplanması, izlenmesi, yorumlanması, kaydedilmesi ve özellik çıkarılması gibi aktiviteleri ifade etmektedir. Bu bilgi içeriğinde sadece video bulunabileceği gibi ayrıca ses, yazı ve doküman imajı gibi bilgiler de bulunabilir.

Yazı Yeniden Yapılandırma: Yazı yeniden yapılandırma, iki birim arasındaki yazılı iletişime ait kimlik bilgisi, durum bilgisi gibi bilgilerin tarafların onayı alınmadan toplanması, izlenmesi, yorumlanması, kaydedilmesi ve özellik çıkarılması gibi aktiviteleri ifade etmektedir. Bu bilgi içeriğinde sadece yazı olabileceği gibi ayrıca ses, video veya doküman imajı gibi bilgiler de bulunabilir [11].

2.2.3 Araya Girme – Değiştirme

Çağrı Karadelik Eylemi: Çağrı karadelik eylemi, VoIP iletişimdeki protokollere ait herhangi bir temel bileşene yetkisiz müdahale edilmesiyle iki taraf arasındaki iletişimin kesilmesini ifade etmektedir.

Çağrı Yeniden Yönlendirme: Çağrı yönlendirme, VoIP iletişimindeki protokollere ait IP veya herhangi bir temel bileşenin yeniden yönlendirilmesi suretiyle çağrının yönlendirildiği aktiviteleri ifade etmektedir.

Faks Değiştirme: Faks değiştirme, faks veya herhangi bir sayısal doküman görselindeki herhangi bir bilginin yetkisiz olarak değiştirilmesini ifade etmektedir.

Konuşma Değiştirme: Konuşma değiştirme; iletişimdeki ses, video ya da herhangi bir bilginin yetkisiz olarak değiştirilmesini ifade etmektedir.

Konuşma Kalitesizleştirme: Çağrı kalitesizleştirme, QoS değerlerinin kasıtlı ve yetkisiz olarak düşürülmesini ifade etmektedir.

Konuşma Taklit ve Ele Geçirme: Konuşma taklit ve ele geçirme eylemi iletişime ait herhangi bir bileşenin ekleme, silme, değiştirme gibi her türlü etkiyle içerik, kimlik ya da durum bilgisi dahil olmak üzere değiştirilmesini ifade eder. Bu içeriklerin türü ses, video, yazı ve/veya imaj olabilir.

Yanlış Arayan Tanımı: Yanlış arayan tanımı, gerçek dışı arayan kimlik bilgisi veya gerçek dışı durum bilgisini ifade etmektedir [11].

2.2.4 Hizmet İstismarı

Çağrı Konferans İstismarı: VoIP çağrı hizmetine ait Çağrı Konferans İstismarı, kimliğin dolandırıcılık amacıyla gizlenmesini ifade etmektedir.

Ödül Oranı Hizmet İstismarı: Ödül Oranı Hizmet İstismarı, trafiğin onay alınmadan ya da faturalandırmanın artırılması dışında bir amaçla yapay olarak artırılmasını ifade etmektedir.

Ödeme için Uygunsuz Atlatma veya Ayarlama: Ödeme için Uygunsuz Atlatma veya Ayarlama eylemi, farklı dolandırıcılık eylemlerini gizlemek için CDR (Call Detail Records – Çağrı Detay Kayıtları) verilerine müdahale edilmesi gibi eylemleri ifade etmektedir [11].

2.2.5 Kasıtlı Hizmet Engelleme

Bu tip tehditler kendi içinde kabaca aşağıdaki gibi sınıflandırılabilir.

- Özel DoS
- Genel DoS
- Fiziksel İhlal
- Kaynak Tükenmesi
- Harici Güç Kaynağının Kaybedilmesi
- Performans Gecikmesi

Detaylandırmak istersek VoIP ağlarına özel DoS saldırıları aşağıda ifade edilebilir.

Talep Sel Saldırıları

- Kullanıcı Çağrı Sel Saldırısı
- Kullanıcıdan Diğer Cihazlara Sel Taşma Saldırısı
- Uç Talep Sel Saldırısı
- Çağrı Kurulumu Sonrası Uç Talep Sel Saldırısı
- Çağrı Kontrol Cihazı Sel Saldırısı
- Talep Döngüsü
- Dizin Hizmeti Sel Saldırısı

Bozuk Talep ve Mesajlar

- Geçersiz Talepler ile Uçbirimin Etkisiz Hale Getirilmesi
- Çağrı İşlemcisine Geçersiz Veri Enjekte Etmek
- Bozuk Protokol Mesajları

QoS Suistimali

Saldırganın, çağrı kurulurken gönderdiği kodek bilgisinden farklı kodek kullanması veya uygulamaya müdahale yoluyla gecikme (latency) oluşturması bu çerçevede değerlendirilebilir.

Sahte mesajlar

Saldırganın araya girerek gönderdiği ve oturumu sonlandırdığı "BYE" mesajı gibi sahte çağrı bitirme mesajları ve "Busy Here" gibi çağrıyı imkânsız kılan cevap mesajları bu çerçevede değerlendirilebilir.

Çağrı Gasbı

Saldırganın bir kullanıcının kayıt (registration) sürecinde protokol paketlerine müdahale ile kullanıcıyı farklı bir uçbirime yönlendirerek kullanıcının istediği çağrıyı kurmasına engel olması, sahte yönlendirme (redirect) mesajıyla ses verisini farklı uçbirime yönlendirmesi veya saldırganın VoIP sunucuyu taklit ederek kullanıcının gerçek sunucuya erişmesini engellemesi bu çerçevede ifade edilebilir.
Ayrıca VoIP özelinde olmayan aşağıdaki DoS saldırı tiplerini de ifade edebiliriz.

- Network Hizmeti DoS Saldırıları
- Altyapıdaki İşletim Sistemlerine ve Bileşenlerine Karşı DoS Saldırıları
- DDoS (Distributed Denial of Service – Dağıtık Hizmet Engelleme Saldırısı) [11]

2.2.6 Fiziksel İhlal

Ağ donanımlarına, ağa ait kablolara ve sistem yazılımlarına fiziksel koşullar içinde yetkisiz ve kötü niyetli müdahaleler bu çerçevede değerlendirilebilir [11].

2.2.7 Diğer Tehditler

Elektrik kesintisi, güç kaynağı yetersizliği, fiziksel kaynakların (hafıza, işlemci) gibi yetersizliği ve kabul edilebilir olmayan gecikme ihtimalleri bu çerçevede değerlendirilebilir [11].

2.3 İLGİLİ ÇALIŞMALAR

VoIP tabanlı sistemlerin tercih edilir hale gelmesiyle birlikte SIP protokolü çoklu ortam iletişim altyapısında standart hale gelmeye başlamış, SIP protokolü ve çevre protokollerinin kullanıldığı sistemler için farklı güvenlik çözümleri önerilmiştir.

VoIP altyapısı güvenliğinden bahsederken bölüm 2.2'de bahsedilen çerçevedeki bütün tehditler üzerine farklı değerlendirmeler ve çalışmalar mevcuttur fakat SIP protokolü özelindeki tehditlerden bahsederken bu çerçevedeki çalışmaların genellikle SIP talep sel saldırıları ve bozuk mesaj kaynaklı DoS saldırılarına odaklandığı söylenebilir.

Örnek çalışmaların tarihçesi aşağıda ifade edilmiştir.

Reynold ve Ghosal, 2003 yılında yapmış olduğu çalışmada SIP sel saldırısına karşı SIP INVITE paketleri ve 200 OK paketleri arasındaki orantıdan faydalandıkları CUSUM (kümülatif toplam) yöntemini önermişlerdir [12]. Wu ve diğ., SIP sel ve SIP akış müdahale saldırılarına karşı SIP ve RTP paketlerinin davranışını inceledikleri SCIDIVE uygulamasını geliştirmişlerdir (2004) [13]. Geneiatakis ve diğ., SIP akış ve SIP mesaj karıştırma saldırısına karşı SIP mesaj yapısını inceledikleri imza tabanlı bir çözüm önermişlerdir (2005) [14]. Chen, çok kaynaklı SIP sel saldırılarına karşı durum makinası çözümü önermiştir (2006) [15]. Niccolini, ilk katmanda mesaj içeriğinin sağlıklı olup olmadığını, ikinci katmanda ise mesaj sırasına bağlı olarak saldırı durumları denetimi için durum makinası kullandığı bir çözümü önermiştir (2006) [16]. Sengar ve diğ., SIP DoS saldırılarını algılamak için, normal protokol davranışı ve anormal davranışı inceledikleri Hellinger Mesafesi tabanlı bir çözüm [17] ve ayrıca durum makinası tabanlı bir çözüm önermişlerdir (2006) [18]. Nassar ve diğ., VoIP ağlarındaki tehditlere karşı Bayes Çıkarım Modeli kullandıkları istatistiksel bir IDS çözümü önermişlerdir (2006) [19]. Rebahi ve Sisalem, CUSUM algoritması ve değişim noktası denetleme yöntemiyle INVITE mesajlarının yoğunluk değişiminin incelendiği bir yöntem önermişlerdir (2007) [20]. Nassar ve diğ., honeypot (balküpü) aracılığıyla normal ve anormal aktivite profillerini ayırarak, farklı profillerin kendi içinde davranış korelasyonlarını incelemişlerdir (2007) [21]. Bouzida ve Mangin, SIP ağına ait belirli parametreleri belirli periyotlarla topladıkları istatiksel verilerle öğrenen bir sistem önermişlerdir (2008) [22]. Rieck ve diğ., anomali tabanlı öğrenen bir sistem önermişlerdir (2008) [23]. Ehlert ve diğ., farklı istatistiksel değerlerin kullanıldığı bir durum makinesi yöntemi önermişlerdir (2008) [24]. Tang ve diğ., Hellinger Mesafesi tabanlı farklı bir

çözüm önermişlerdir (2009) [25]. Nassar ve diğ., saldırı tipini belirlemek ve saldırı kaynağını tespit etmek için Opensips SIP sunucuya ait 38 adet istatistiksel veri ile makine öğrenme algoritması olarak SVM (Support Vector Machine – Destek Vektör Makineleri) algoritmasından faydalandıkları bir çözüm önerdiler (2010) [26]. Aziz ve Gul, bozuk biçimli SIP mesajı saldırılarına karşı iki-gram tabanlı öğrenen bir sistem önerdiler (2010) [27]. Nassar ve diğ., makine öğrenmesi kullanan sistemlerin eğiticili algoritmaları için kullanabileceği temel ihtiyaç olan etiketli veri setini üretmek amacıyla bir laboratuvar ortamı kurmuş ve ürettikleri verileri yayınlamış (2010) [28] ayrıca VoIP altyapısı için risk yönetimi amacıyla SVM'den faydalanmışlardır (2010) [29]. Ferdous ve diğ., ilk aşamada söz dizimi kontrolü ve ikinci aşamada SVM kullandıkları bir güvenlik çözümü geliştirmişlerdir (2012) [30]. Fakis ve diğ., makine öğrenmesinin SIP DDoS saldırılarını denetlemede başarı düzeyini incelemek için beş farklı makine öğrenme algoritmasını test etmişlerdir (2015) [31]. Taş ve diğ., SIP DDoS saldırılarını engellemek amacıyla SIP paket sayıları için eşik değer tabanlı bir çözüm önermişlerdir (2016) [32]. Yıldız ve diğ., SIP ağlarındaki trafiğin benzetimi amacıyla olasılıksal bir SIP trafik benzetim aracı geliştirmişlerdir (2018) [33]. Kurt ve diğ., SIP DDoS saldırı tespiti için belirli periyotlarla elde edilen anlık SIP paket adetlerini kullanan Bayesci Değişim Noktası tabanlı bir çözüm önermişlerdir (2018) [34].

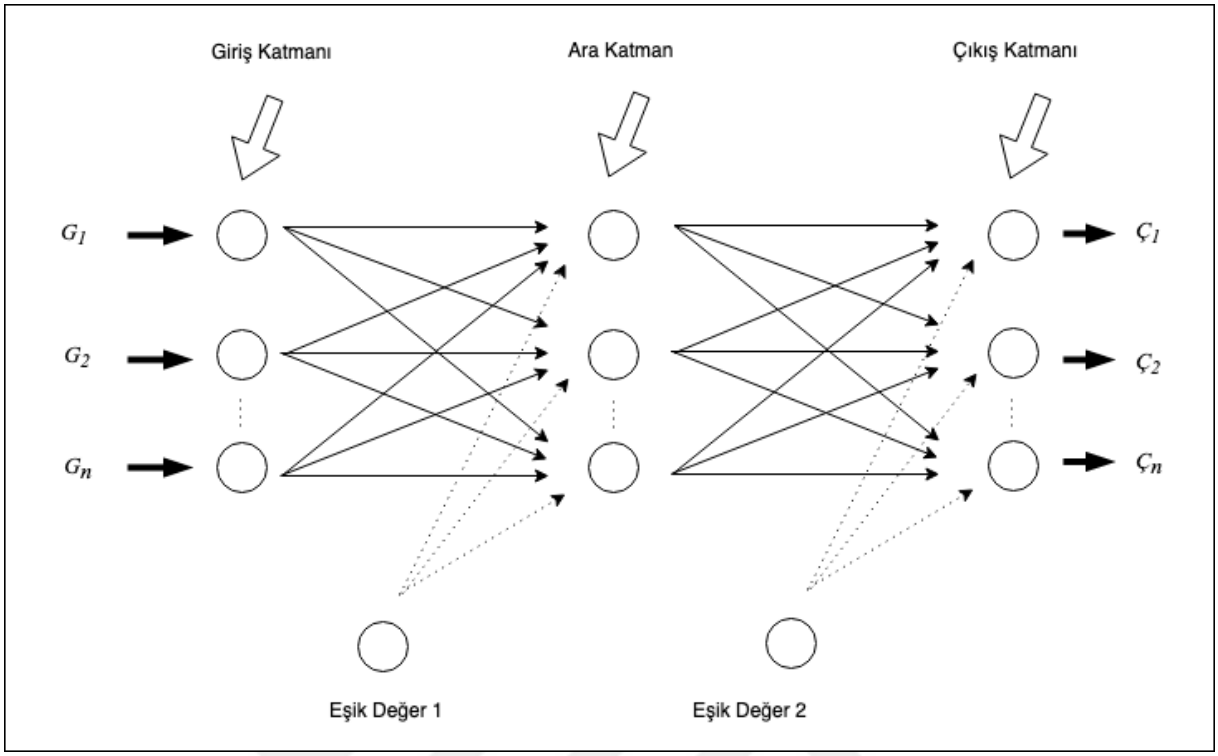
VoIP izleme sistemlerinde ayrıca uçtan uca çözüm bağlamında makine öğrenmesi, QoS gibi konularda da önerilmiştir. Örnek olarak Chi ve Womack, ses kalitesini belirlemek için SVR (Support Vector Regression – Destek Vektör Regresyonu) tabanlı bir yöntem önermişlerdir (2009) [35]. Larijani ve Radhakrishnan ise ses kalitesini belirlemek için girdi olarak gecikme, gecikme değişimi ve paket kaybını kullanan RNN (Random Neural Network – Rastgele Sinir Ağı) (2010) [36] [37] tabanlı çözümler önermişlerdir.

2.4 KULLANILAN ALGORİTMALAR

2.4.1 MLP

Yapay sinir ağları, insan beyninin öğrenme ve çıktı üretme sürecindeki mekanizması temel alınarak farklı amaçlar doğrultusunda benzer eylemleri gerçekleştirmek üzere geliştirilen yazılımsal yapılardır.

MLP ağlarında yapı, bu amaçları gerçekleştirmek üzere birden fazla katmandan oluşmaktadır. Ağın mimarisine bağlı olarak nöronlar farklı şekilde birbirine bağlı olabilir.



Şekil 2.6: Temel MLP ağ yapısı.

MLP ağlarında bilgi bu ağı oluşturan yapay sinir hücresindeki ağırlıkla temsil edilmektedir. Öğrenme ise algoritmaya bağlı olarak bu ağırlıkların güncellenmesidir. MLP, eğiticili yapay öğrenme yöntemleri arasında yer almaktadır. Öğrenme esnasında her bir tekrarda giriş katmanındaki her bir sinir hücresine belirli birer öznitelik bilgisi iletilir. Çıkış katmanı istenilen sınıf bilgisini verene kadar algoritmaya bağlı ağırlık değerleri sürekli güncellenir. MLP ağlarında giriş katmanı, en az bir ara katman ve çıkış katmanı olmak üzere asgari üç katman olmak zorundadır.

Genel bir MLP ağ yapısı Şekil 2.6'da verilmiştir.

MLP'de giriş katmanında bilgi işlenmez. Buradaki bilgiler işlenmek üzere sonraki katmandaki tüm yapay sinir hücrelerine iletilir.

Yapay sinir ağındaki her bir sinir hücresi 5 adet bileşenden oluşur.

Bunlar sırasıyla; girdiler, ağırlıklar, birleştirme fonksiyonu, aktivasyon fonksiyonu ve çıktı bilgileridir.

Girdiler

Yapay sinir hücresine dış dünyadan iletilen bilgilerdir.

Ağırlıklar

Sinir hücrelerindeki ağırlıklar dışarıdan gelen bilginin sınıf belirlenme sürecindeki önem değerini belirler ve öğrenme süreci boyunca bu değerler, ağ doğru sınıf bilgisini üretene kadar yeniden hesaplanır.

Birleştirme fonksiyonu

Burada yapay sinir hücresine dışarıdan gelen net girdi hesaplanır. En yaygın kullanılan birleştirme fonksiyonunda, girdiler ağırlıklarıyla çarpılarak tek bir sinir hücresi için toplamı hesaplanır.

$$\text{NET} = \sum_{i}^{n} G_i \, A_i \tag{2.1}$$

Aktivasyon fonksiyonu

Burada yapay sinir hücresine gelen net girdi işlenir ve tercih edilecek fonksiyona bağlı olarak nasıl bir çıktı üretileceği belirlenir. MLP ağında aktivasyon fonksiyonu olarak genellikle sigmoid fonksiyonu kullanılmaktadır.

$$F(NET) = \frac{1}{1 + e^{-NET}} \tag{2.2}$$

Çıktı

Çıktı, ilgili sinir hücresinin aktivasyon fonksiyonu sonucunda ürettiği değerdir. Bu bilgi ağın yapısı ve yapay sinir hücresinin konumuna bağlı olarak ya dış dünyaya, ya da diğer hücrelere iletilir.

Bir MLP ağının karakteristik özelliklerini aşağıdaki parametreler belirler.

- Ağ yapısı
- Birleştirme fonksiyonu

- Aktivasyon fonksiyonu
- Tercih edilen öğrenme stratejisi
- Tercih edilen öğrenme kuralı

MLP ağının öğrenme kuralı en küçük kareler toplamına dayanan Delta Öğrenme Kuralının genelleştirilmiş halidir. Bu sebeple bu kural Genelleştirilmiş Delta Kuralı şeklinde de ifade edilmektedir.

Delta kuralını oluşturan iki safha aşağıdaki gibidir.

1. İleriye doğru hesaplama: Bu safhada ağın çıktısı hesaplanır.
2. Geriye doğru hesaplama: Bu safhada ağırlıklar güncellenir.

İleri doğru hesaplama yapılırken girdi katmanında işlem yapılmaz. Bu sebeple giriş katmanındaki her bir işlem elemanının çıktısı aşağıdaki şekilde belirlenir.

$$Ç_k^i = G_k \tag{2.3}$$

Ara katmanlardaki sinir hücreleri için; ağırlıklar (*A1, A2...*) olmak üzere net girdi;

$$NET_j^a = \sum_{k=1}^{n} A_{kj}\, Ç_k^i \tag{2.4}$$

şeklinde hesaplanır.

Aktivasyon fonksiyonu olarak eğer sigmoid fonksiyonu tercih edilirse çıktı;

$$Ç_j^a = \frac{1}{1 + e^{-NET_j^a - \beta_j^a}} \tag{2.5}$$

şeklinde ifade edilebilir.

Burada β değeri 1 olmak üzere eşik değerini ifade etmektedir. Bu değer eğitim süresince değişmez.

Geriye doğru hesaplama yapılırken (*B1, B2...*) beklenen çıktılar olmak üzere, çıktılar bu değerlerle karşılaştırılır. Beklenen değer ve çıktı arasındaki fark hata kabul edilir. Hata değerini

azaltmak için; bu değer her bir iterasyonda MLP ağının ağırlık değerlerine dağıtılmak suretiyle ağ yapısı güncellenir.

Çıktı katmanındaki $n.$ yapay sinir hücresi için hata E_n olmak üzere;

$$E_n = B_n - Ç_n \tag{2.6}$$

şeklinde ifade edilebilir. Bir yapay sinir hücresine ait toplam hata aşağıdaki formülle hesaplanır.

$$\text{TH} = \frac{1}{2}\sum_m E_m^2 \tag{2.7}$$

Toplam hatanın asgariye indirilmesi için bu hata kendisine sebep olan sinir hücrelerine dağıtılır.

Ara katman ve çıktı katmanı arasındaki ağırlıkları değiştirirken ara katmandaki j. yapay sinir hücresini çıktı katmanındaki m. sinir hücresine bağlayan bağlantı ağırlığının ne kadar değişeceği ΔA^a t. iterasyonda aşağıdaki gibi hesaplanır;

$$\Delta A_{jm}^a(t) = \lambda \delta_m Ç_j^a + \alpha \Delta A_{jm}^a(t-1) \tag{2.8}$$

λ burada öğrenme katsayısını ifade etmektedir. Öğrenme katsayısı ağırlıkların değişim miktarını belirler. Burada ağırlıkları değiştirirken değişimin yerel bir optimuma takılmaması için, değişimin değerinin belirli bir oranda sonraki iterasyonda eklenmesi sağlanır. Bu değişime momentum denir. Momentum katsayısı, α ile ifade edilir.

Eşitlikteki δ_m ise m. no'lu çıktı yapay sinir hücresinin hatasını ifade eder ve aşağıdaki şekilde hesaplanır;

$$\delta_m = f'(NET).E_m \tag{2.9}$$

Burada aktivasyon fonksiyonun türevi $f'(NET)$ şeklinde ifade edilmiştir. Aktivasyon fonksiyonu olarak sigmoid fonksiyonu kullanıldığında;

$$\delta_m = Ç_m(1 - Ç_m).E_m \tag{2.10}$$

şeklinde hesaplanır.

Değişim miktarı hesaplandıktan sonra ağırlıklar $t.$ iterasyonda aşağıdaki şekilde güncellenir.

$$A_{jm}^{a} = A_{jm}^{a}(t-1) + \Delta A_{jm}^{a}(t) \quad (2.12)$$

Çıktı katmanındaki yapay sinir hücrelerinin eşik değer ağırlıklarını $\beta^{ç}$ ile ifade edecek olursak; bu birimin değişim miktarı aşağıdaki şekilde hesaplanır.

$$\Delta\beta_{m}^{ç}(t) = \lambda\delta_{m} + \alpha\Delta\beta_{m}^{ç}(t-1) \quad (2.13)$$

Eşik değerin t. iterasyondaki ağırlık değeri ise;

$$\beta_{m}^{ç}(t) = \beta_{m}^{ç}(t-1) + \Delta\beta_{m}^{ç}(t) \quad (2.14)$$

şeklinde hesaplanır.

Giriş katmanı ve ara katman arasındaki veya ara katmanlar arasındaki ağırlıkların değişimi, ΔA^{i} ile gösterildiğinde değişim miktarı;

$$\Delta A_{kj}^{i}(t) = \lambda\delta_{j}^{a}Ç_{k}^{i} + \alpha\Delta A_{kj}^{i}(t-1) \quad (2.15)$$

olacaktır.

Burada hata terimi δ^{a} şeklinde ifade edilmek üzere aşağıdaki şekilde hesaplanır;

$$\delta_{j}^{a} = f'(NET)\sum_{m}\delta_{j}\ A_{j}^{m} \quad (2.16)$$

Aktivasyon fonksiyonu olarak eğer sigmoid fonksiyonu tercih edilirse hata değeri aşağıdaki şekilde olur;

$$\delta_{j}^{a} = Ç_{j}^{a}\left(1 - Ç_{j}^{a}\right).\sum_{m}\delta_{m}A_{jm}^{a} \quad (2.17)$$

Bu formüle göre değişim miktarı hesaplandıktan sonra ağırlıklar aşağıdaki şekilde hesaplanır;

$$A_{kj}^{i}(t) = A_{kj}^{i}(t-1) + \Delta A_{kj}^{i}(t) \quad (2.18)$$

Ara katman eşik değerleri β^{a} ile gösterilirse değişim miktarı aşağıdaki şekilde olur;

$$\Delta\beta_j^a(t) = \lambda\delta_j^a + \alpha\Delta\beta_j^a(t-1) \tag{2.19}$$

t. iterasyonda ağırlıklar aşağıdaki şekilde hesaplanır;

$$\beta_j^a(t) = \beta_j^a(t-1) + \Delta\beta_j^a(t) \tag{2.20}$$

Sırasıyla ileri ve geriye doğru hesaplama adımları, beklenen çıktılar oluşana kadar devam ettirilerek eğitim süreci tamamlanır [38].

2.4.2 NB (Naive Bayes – Naif Bayes)

İstatistiksel bir sınıflandırma yöntemi olan NB sınıflandırıcıda amaç belirli bir örnek kümesi içinde bir örneğin, bir sınıfa ait olmasının koşullu olasılıklarını değerlendirmektir. X sınıfı bilinmeyen bir veri örneği olmak üzere, $X = \{x_1, x_2 \ldots x_n\}$ nitelik değerlerinden oluştuğunu kabul edelim. Bu örnek sınıfta m adet sınıf olduğunu varsaydığımızda $C_1 \ldots C_n$ sınıf değerleri olmak üzere sınıfı belirlenecek bir örnek için öncelikle (2.21)'de gösterildiği şekilde olasılık değerleri hesaplanır.

$$P(C_i|x) = \frac{P(X|C_i)P(C_i)}{P(x)} \tag{2.21}$$

Hesaplamalarda işlem yükünü azaltmak amacıyla $P(X|C_i)$ olasılığı basitleştirilebilir. Bunun için x_i değerleri birbirinden bağımsız kabul edildiğinde (2.22)'te gösterilen bağıntı kurulabilir.

$$P(X|C_i) = \prod_{k=1}^{n} P(Xk|C_i) \tag{2.22}$$

Sınıfını bilmediğimiz bir X örneğini sınıflandırmak için (2.21)'de $P(C_i \mid X)$ içinde yer alan payda değerleri eşit olduğundan, pay değerleri karşılaştırılıp mevcut değerler içinden büyük olan seçilerek bilinmeyen örneğin bu sınıfa ait olduğu ifade edilebilir.

$$arg\ max_{c_i} = \{P(X|C_i)P(C_i)\} \tag{2.23}$$

Bu ifade (2.23), MAP (Maximum A Posteriori Classification – En Büyük Sonrasal Sınıflandırma) yöntemi olarak ta bilinmektedir.

$$C_{MAP} = \arg\max_{c} \prod_{k=1}^{n} P(Xk|C_i) \quad (2.24)$$

Bu durumda (2.22)'den dolayı yukarıdaki bağıntı (2.24) NB sınıflandırıcı olarak kullanılabilir [39].

3. MALZEME VE YÖNTEM

Çalışmada kullanıcı davranışı ve saldırı benzetimi yapmak, daha sonra ise ilgili değerleri sınıflandırmak için belirli bileşenlerden faydalanılmıştır. Ayrıca bu benzetim neticesinde sunucu değerlerini anlık takip eden ve saldırı durumunu tercih edilen algoritma doğrultusunda değerlendiren bir uygulama prototipi geliştirilmiştir. Benzetim detayları bölüm 3.1'de, uygulama detayları ise bölüm 3.2'de ifade edilmiştir.

3.1 SİMULASYON

3.1.1 BOUN-SIM

Boun-Sim uygulaması Yıldız ve diğ. tarafından daha önce başka bir akademik çalışmanın konusu olarak SIP çağrı benzetimi amacıyla geliştirilmiş; ayrıca Bayesci Değişim Noktası algoritmasının DDoS saldırılarının tespitinde başarı düzeyini değerlendirmek amacıyla kullanılmıştır [33][34]. Bu çalışmada testlerin gerçekleştiği süreçte, bahsedilen uygulamaya ait erişilebilir olan sanal makine ve açık kaynak uygulama kodlarından faydalanılmıştır [40]. Uygulama bileşenleri aşağıdaki gibidir.

Simulator: Maksimum 6 adet kullanıcı bilgisi ile, verilen parametreler doğrultusunda IP bilgileri verilen PS üzerinde olağan SIP trafik benzetimi yapmaktadır.

Attacker: Verilen parametreler doğrultusunda IP bilgileri verilen hedef PS üzerinde belirli yoğunlukta SIP trafiği oluşturmaktadır. Bu yükün oluşma süreci Wireshark uygulaması ile test edildi. Saldırı benzetimi için bu uygulamaya ait betik kodlarından faydalanıldı.

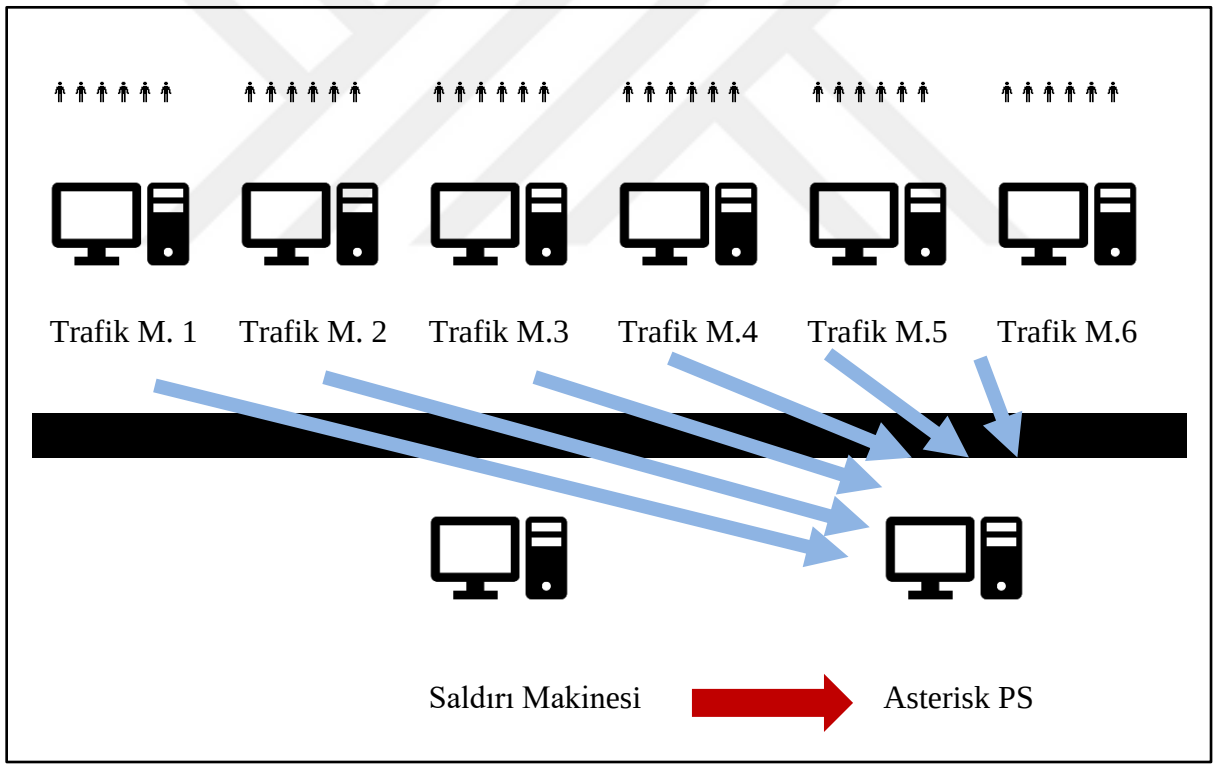
Monitor: Bu uygulama sunucu ve istemci olmak üzere iki parçadan oluşmaktadır. Sunucu, testlerin yapılacağı PS üzerinden gerekli parametreleri toplayıp istemci tarafına iletmek için bir soket bağlantısı oluşturmakta ve belirli periyotlarla bu bilgileri istemciye iletmektedir. Uygulama sunucu ve istemci olmak üzere "boun_server.py" ve "boun_client.py" bileşenlerine sahiptir.

Eğer uygulamaya parametre olarak bir log dosyası verilirse, uygulama tarafından alınan değerler istemci tarafında bir log dosyasında muhafaza edilebilmektedir.

Test sürecinde i7 işlemci ve 32 GB RAM (Random Access Memory – Rastgele Erişimli Bellek)'e sahip bir bilgisayar kullanıldı. Bu cihazda test amaçlı trafik oluşturmak üzere simulator uygulamasının yüklü olduğu 6 adet Ubuntu sanal makine konumlandırıldı. Bir adet Ubuntu sanal makine saldırı aracını kullanmak üzere, bir adet Ubuntu sanal makine ise süreci yönetmek üzere operatör olarak oluşturuldu. Tüm trafik sanal makineler üzerinde ev sahibi makine üzerinden sanal ağ vasıtası ile yönetildi. Bir adet sanal makinede ise Asterisk PS konumlandırıldı. Benzetim için organize edilen topoloji Şekil 3.1'de görselleştirilmiştir.

3.1.2 Trixbox

PS ihtiyacı için Trixbox dağıtımı kullanıldı. Trixbox dağıtımı, içerisinde Asterisk PS ve belirli VoIP uygulamalarını barındırmaktadır [41].



Şekil 3.1: Benzetim şeması.

Test sürecinde altı adet sanal makine (Trafik M.1 – Trafik M.6) her biri bağımsız olarak altı adet kullanıcının yapabileceği trafiğin benzetimini yaptılar. Bu trafiğe ait anlık mesaj histogram verileri kaydedildikten sonra, trafik devam ederken ayrıca bir adet makineden de farklı yoğunlukta SIP paketleri gönderilerek DoS saldırıları altında değerlendirilen SIP sel

saldırıları yapıldı. Bu saldırılarda PS üzerine farklı yoğunluklarda INVITE ve REGISTER mesajları yönlendirildi. Mesaj yoğunluğunun artırılması için betiklerde her bir iterasyon için mesaj gönderilecek kullanıcı sayısı artırıldı. Saldırı sürecinde elde edilen anlık mesaj histogramları, her bir profil için ayrıca kaydedildi.

Daha sonra elde edilen veriler sırası ile; saldırı içermeyen ve "0" ile etiketlenmiş yaklaşık 15 dakika boyunca toplanan 600 örnek, saldırı içeren ve "1" ile etiketlenmiş 240 örnek tek bir CSV (Comma Separated Values – Virgülle Ayrılmış Değerler) dosyasında her bir saldırı profili için ayrı ayrı olmak üzere 12 dosya olarak Python betikleri aracılığıyla birleştirildi. Bu veriler ayrıca Weka uygulaması vasıtasıyla önce normalize edildi, daha sonra MLP ve NB algoritmaları ile test edildi. Test sonuçları bölüm 4'te ifade edilmiştir.

Her bir iterasyon için SIP mesaj tipi ve kullanıcı sayısına bağlı olarak benzetimi yapılan SIP sel saldırılarının anlık yükleri yaklaşık olarak Tablo 3.1 ve Tablo 3.2'de ifade edilmiştir.

Tablo 3.1: INVITE sel saldırılarında üretilen yaklaşık anlık paket yükü.

INVITE x 5	1,69 paket/sn
INVITE x 10	3,26 paket/sn
INVITE x 20	6,6 paket/sn
INVITE x 50	16,31 paket/sn
INVITE x 100	24,70 paket/sn
INVITE x 500	56,25 paket/sn

Tablo 3.2: REGISTER sel saldırılarında üretilen yaklaşık anlık paket yükü.

REGISTER x 5	3,75 paket/sn
REGISTER x 10	8,58 paket/sn
REGISTER x 20	13,52 paket/sn
REGISTER x 50	41,38 paket/sn
REGISTER x 100	47,43 paket/sn
REGISTER x 500	81,38 paket/sn

3.1.3 Weka

Weka uygulaması Yeni Zelanda Waikato Üniversitesi tarafından geliştirilmiş, farklı makine öğrenmesi tekniklerinin kolaylıkla kullanılmasını sağlayan açık kaynaklı bir uygulamadır [42]. Bu çalışmada benzetim sürecinde elde edilen veriler Python betikleriyle işlenebilir hale getirildikten sonra sınıflandırma sürecinde Weka uygulamasının kullanımı tercih edilmiştir.

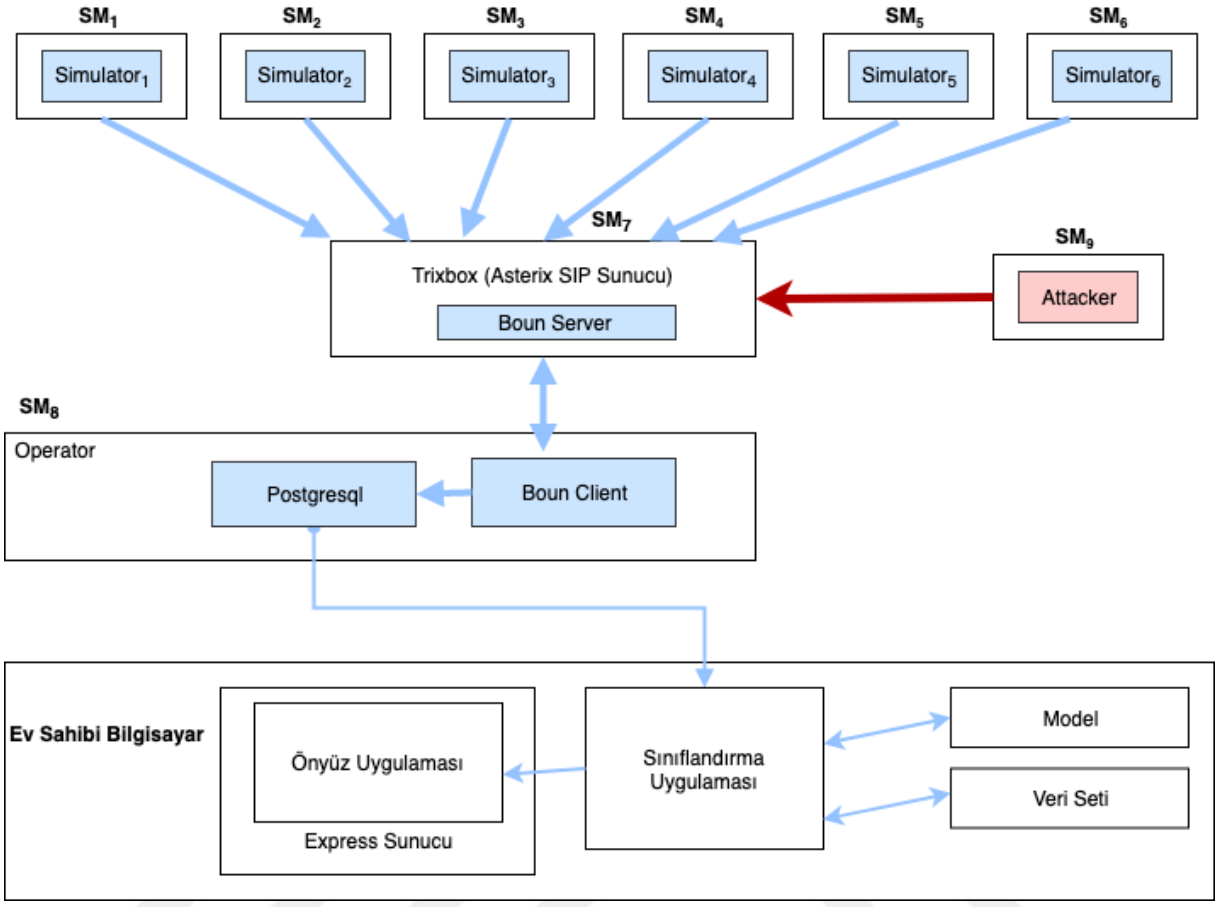
Burada Python betikleriyle oluşturulan dosyalardaki veriler CSV formatındadır. Çalışmada öncelikle bu dosyalardaki veriler sınıflandırma algoritmalarını test etmek amacıyla Weka yazılımına yüklendi. Daha sonra veriler bu uygulama vasıtasıyla normalize edildi ve sınıf değişkeni nominal hale getirilerek sınıflandırma algoritmalarında kullanıma hazır hale getirildi. Test edilen verilere ait değerler ve çalışma detayları bölüm 4'te anlatılmıştır.

3.2 GELİŞTİRİLEN UYGULAMA

Çalışma sürecinde yapmış olduğumuz benzetimler neticesinde test ettiğimiz makine öğrenmesi algoritmalarının ümit verici başarı düzeyi üzerine çalışmanın çevrimiçi bir izleme uygulaması prototipine dönüştürülmesi değerlendirildi. Bu uygulamanın geliştirilme sürecinde daha önce benzetim sürecinde elde edilen etiketli veriler ve eğitim sırasında elde edilen modelden faydalanıldı. Çalışma sürecinde oluşturulan uygulama ortamı ve mimarisi Şekil 3.2'de görselleştirilmiştir. Uygulama test edilirken yine benzetim sürecinde kullandığımız sanal makinalardan (SM_1 ve SM_9 arasında) faydalanıldı.

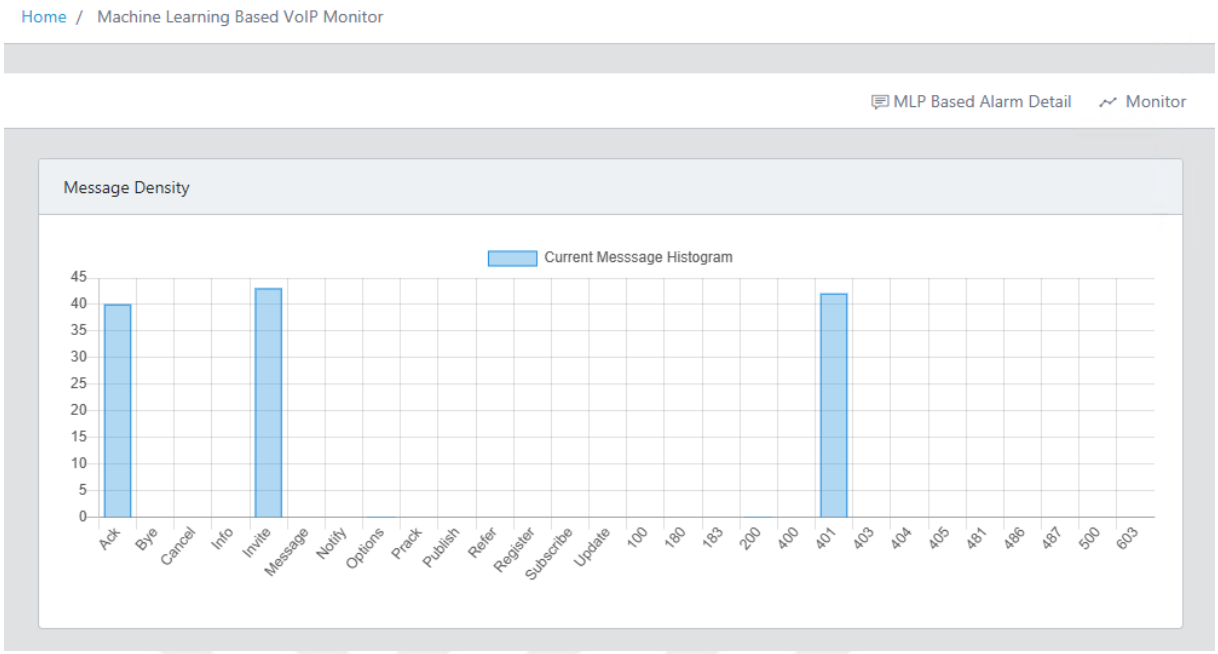
Geliştirdiğimiz uygulama Boun-Sim üzerinde belirli geliştirmeler yapılarak, ayrıca bir mikro servis ve bir adet te önyüz çalışması yapılarak geliştirildi. Bu önyüz uygulamasına ait anlık mesaj yoğunluğu grafiği Şekil 3.3'te, genel parametre izleme grafikleri Şekil 3.4'te, makine öğrenmesine bağlı alarm takip ekran görüntüsü Şekil 3.5'te gösterilmiştir.

Çalışmada PS'a ait verileri tutmak amacıyla Boun-Client uygulamasının olduğu sanal makinaya -tüm işlemleri yönettiğimiz sanal makine (SM_8)- bir adet Postgresql 9 veritabanı kuruldu. Boun-Sim uygulamasının bileşeni olan "boun_client.py" betiği aracılığıyla gelen her soket paket içeriğinin bu veritabanına kaydedilmesi sağlandı. Ev sahibi bilgisayarda ise Java diliyle bir adet mikro servis uygulaması geliştirildi. Bu mikro servis uygulamasına Weka uygulama kütüphaneleri kullanılarak sınıflandırma özelliği entegre edildi. Uygulamaya entegre edilen önyüz uygulamasında Angular önyüz uygulama iskeleti (framework) kullanıldı.

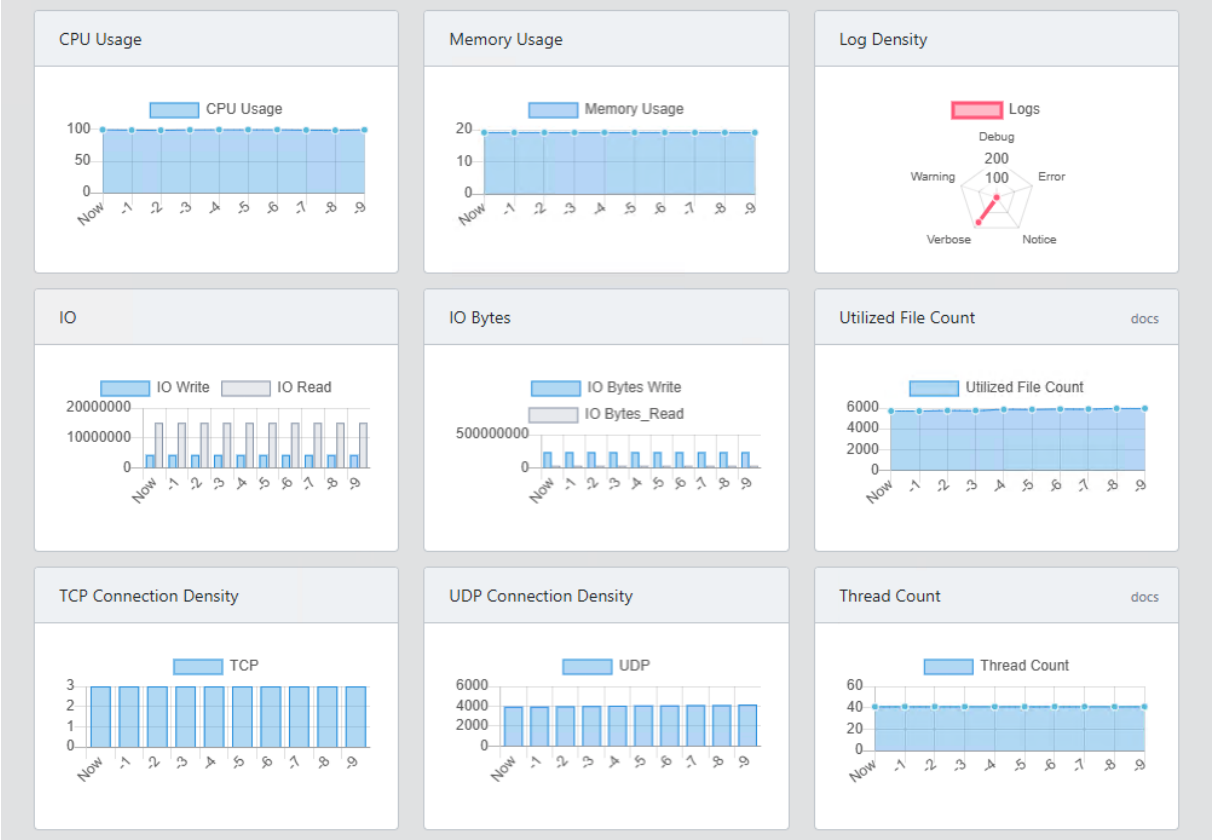


Şekil 3.2: Uygulama benzetim mimarisi.

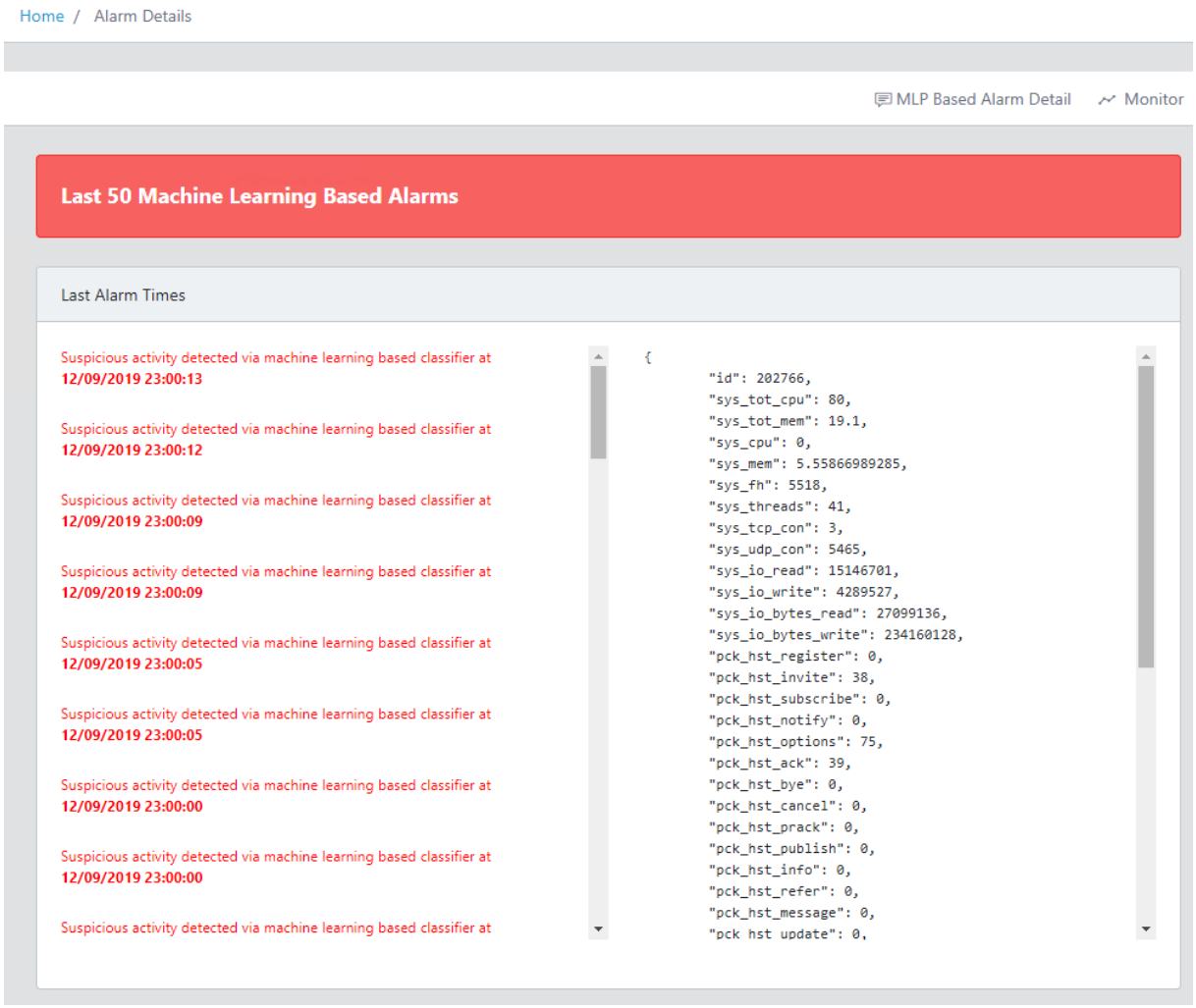
Grliştirdiğimiz uygulama belirli periyotlarla REST (Representational State Transfer – Temsili Durum Aktarımı) servis aracılığıyla veritabanındaki son verileri JSON (JavaScript Object Notation – JavaScript Nesne) formatında alıp, tarayıcı tarafında izlenebilir hale getirmektedir. Her bir REST çağrısında son 10 veri incelenmektedir. Bu süreçte veriler, daha önce işlenen veri seti dikkate alınarak normalize edilmekte, ayrıca daha önce oluşturulan model dikkate alınarak sınıf bilgisi MLP algoritmasına göre sınıflandırılmaktadır. Pozitif sınıflanan veriler ise veritabanında işaretlenmekte ve önyüzde alarm bilgisi olarak sunulmaktadır. Önyüzde Core UI Angular şablon uygulamasından faydalanılmıştır [43]. Sınıflandırma uygulaması geliştirilirken Emara tarafından yazılan kodlardan faydalanılmıştır [44]. Çalışma normal SIP trafiği benzetimi ve saldırı trafiği benzetimi yapılarak test edilmiştir.



Şekil 3.3: Uygulamaya ait anlık mesaj yoğunluğu görüntüsü.



Şekil 3.4: Uygulamaya ait parametre izleme grafikleri.

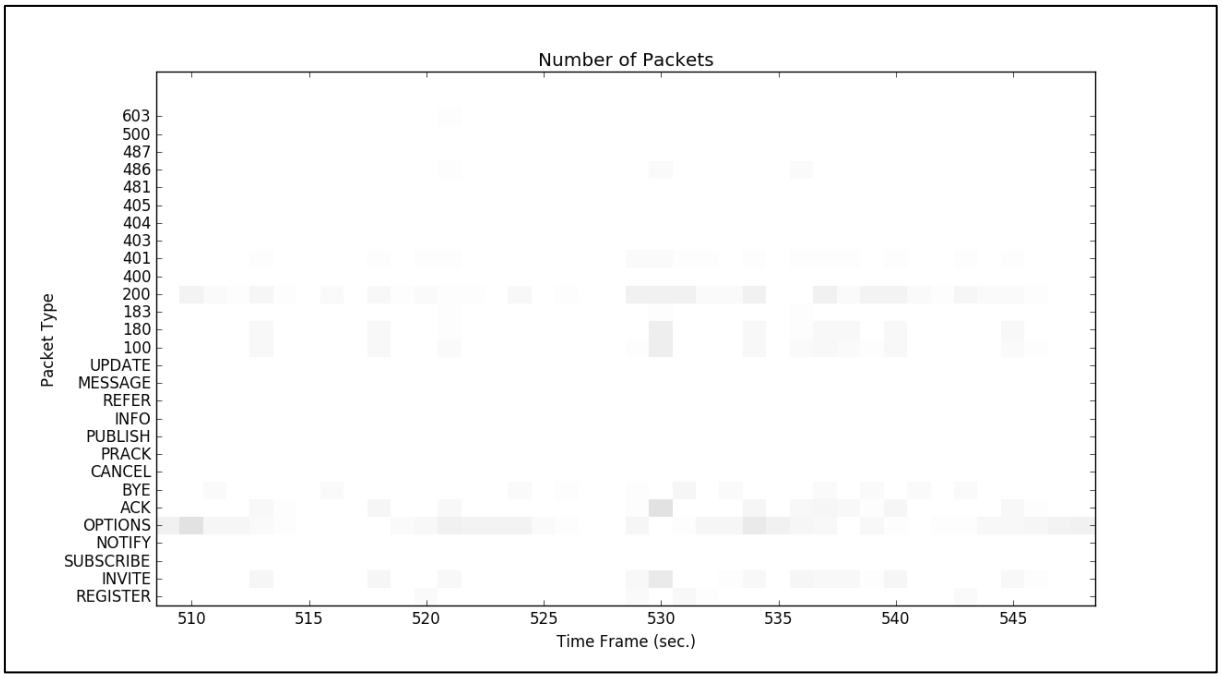


Şekil 3.5: Uygulamaya ait alarm takip ekranı.

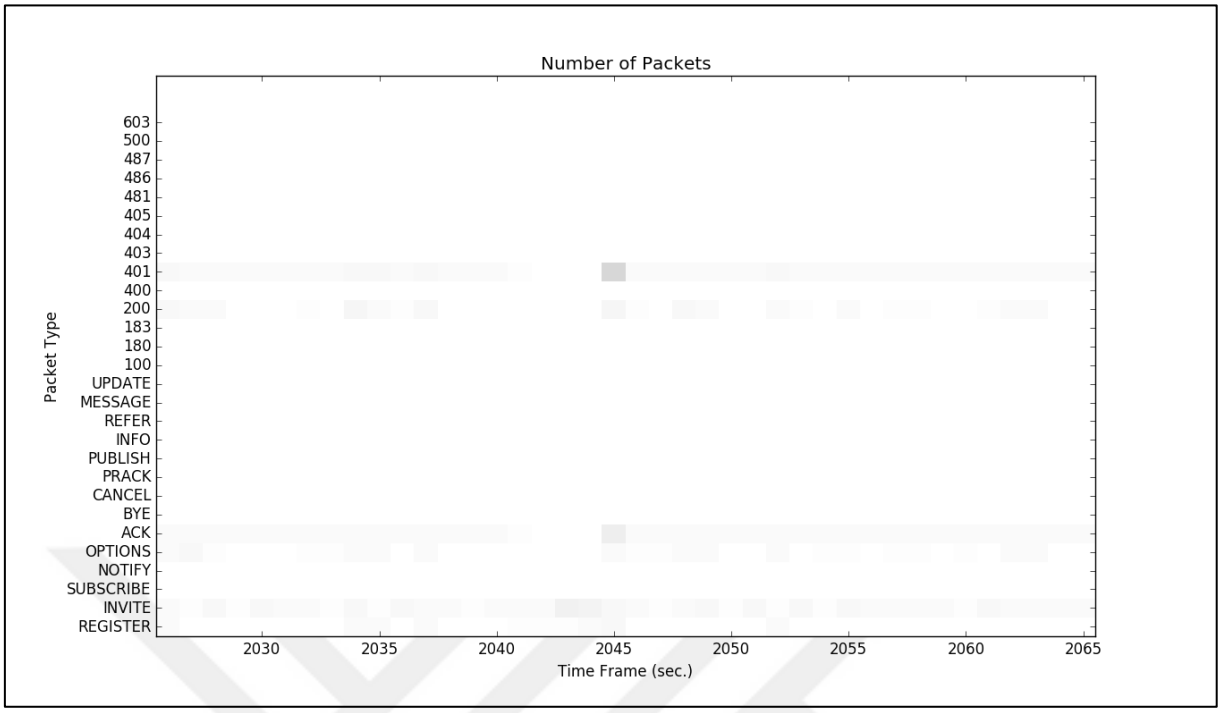
4. BULGULAR

Mevcut benzetim düzeneğinde 6 adet sanal makine aracılığıyla, her bir makinede 6 adet kullanıcı benzetimi yapılarak önce PS üzerinde arka plan trafiği oluşturuldu ve bu değerler saldırısız ortamı ifade eden "0" etiketiyle etiketlendi. Daha sonra ise bu arka plan trafiği devam ederken her bir iterasyon için sırasıyla 5, 10, 20, 50, 100 ve 500'er adet kullanıcı olmak üzere SIP (INVITE) ve daha sonra aynı adetler olmak üzere SIP (REGISTER) mesajlarıyla farklı bir sanal makine üzerinden PS'a doğru SIP DoS saldırıları yapıldı. Bu aşamada elde edilen veriler ise saldırı durumunu ifade eden "1" ile etiketlendi. Sınıflandırma amacıyla veri kümesi olarak ise SIP paketlerine ait histogram verileri kullanıldı. Çalışmada öncelikle loglanan verilerin sınıflandırma başarısını test etmek için MLP ve NB algoritmaları değerlendirildi. Verilerin bu algoritmalar ile test edilmesi için, veriler öncelikle CSV formatına çevrildi. Daha sonra veriler normalize edildi ve sınıf bilgisi nominal hale getirildi. Daha sonra bu veriler Weka aracı vasıtasıyla MLP ve NB algoritmaları ile test edildi. Benzetim sürecinde Boun-Sim Monitor uygulaması tarafından elde edilen, ilgili trafiğe ait ısı haritaları Şekil 4.1 – Şekil 4.13 arasında, test sonuçları ise Tablo 4.1 – Tablo 4.12 arasında gösterilmiştir.

Çok katmanlı algılayıcıda öğrenme oranı: 0.3, momentum: 0.2 ve öğrenme zamanı 1000 seçildi.



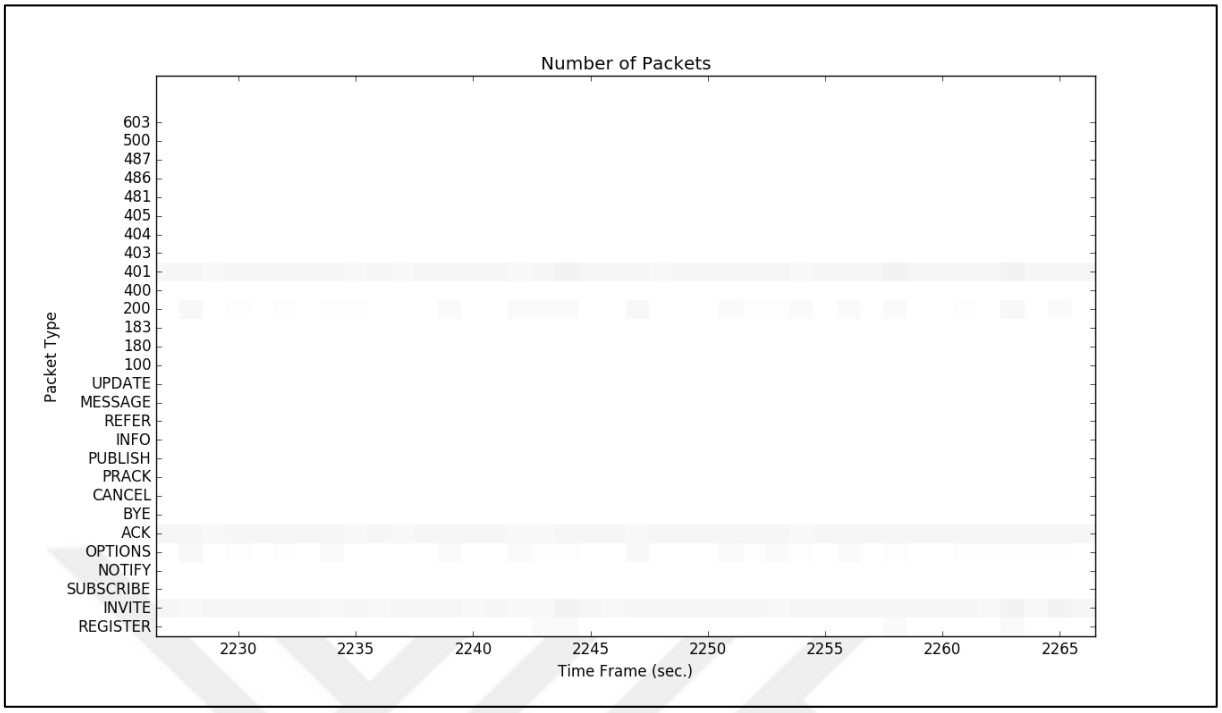
Şekil 4.1: Sadece arka plan trafiğine ait ısı haritası.



Şekil 4.2: 5 x INVITE mesajı ile ısı haritası.

Tablo 4.1: 5 INVITE paketi yük yoğunluğuna bağlı başarı değerleri.

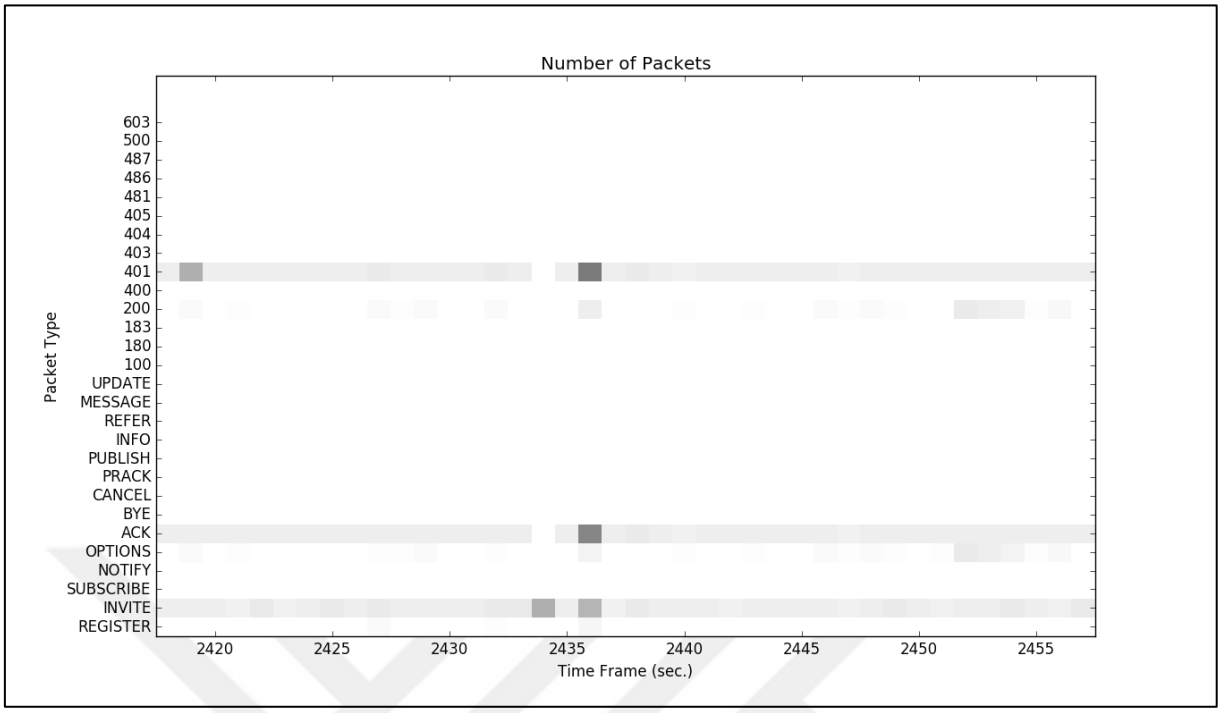
Algoritma	**Başarı Düzeyi**	
NB	Doğruluk:	%83.5714
	Hassasiyet (Precision):	0.925
	Kesinlik (Recall):	0.463
	F-Skoru:	0.617
MLP	Doğruluk:	%96.5476
	Hassasiyet (Precision):	0.920
	Kesinlik (Recall):	0.963
	F-Skoru:	0.941



Şekil 4.3: 10 x INVITE mesajı ile ısı haritası.

Tablo 4.2: 10 INVITE paketi yük yoğunluğuna bağlı başarı değerleri.

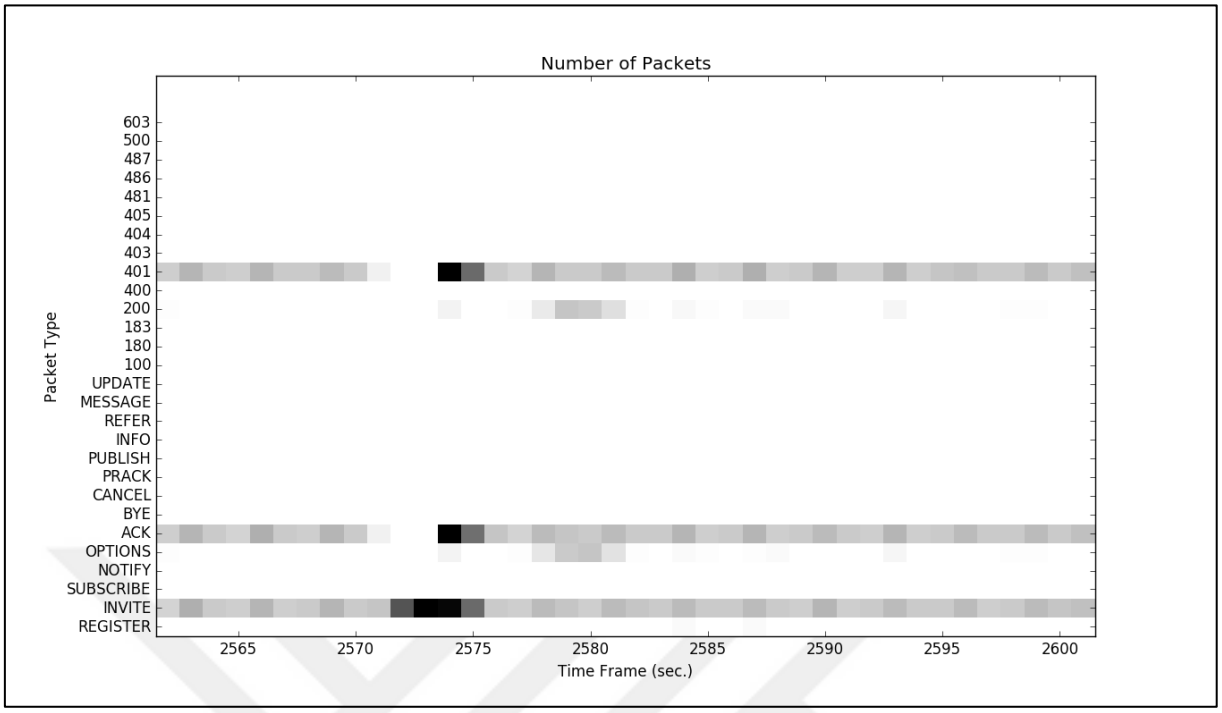
Algoritma	**Başarı Düzeyi**	
NB	Doğruluk:	%94.7619
	Hassasiyet (Precision):	0.868
	Kesinlik (Recall):	0.963
	F-Skoru:	0.913
MLP	Doğruluk:	%99.2857
	Hassasiyet (Precision):	0.983
	Kesinlik (Recall):	0.992
	F-Skoru:	0.988



Şekil 4.4: 20 x INVITE mesajı ile ısı haritası.

Tablo 4.3: 20 INVITE paketi yük yoğunluğuna bağlı başarı değerleri.

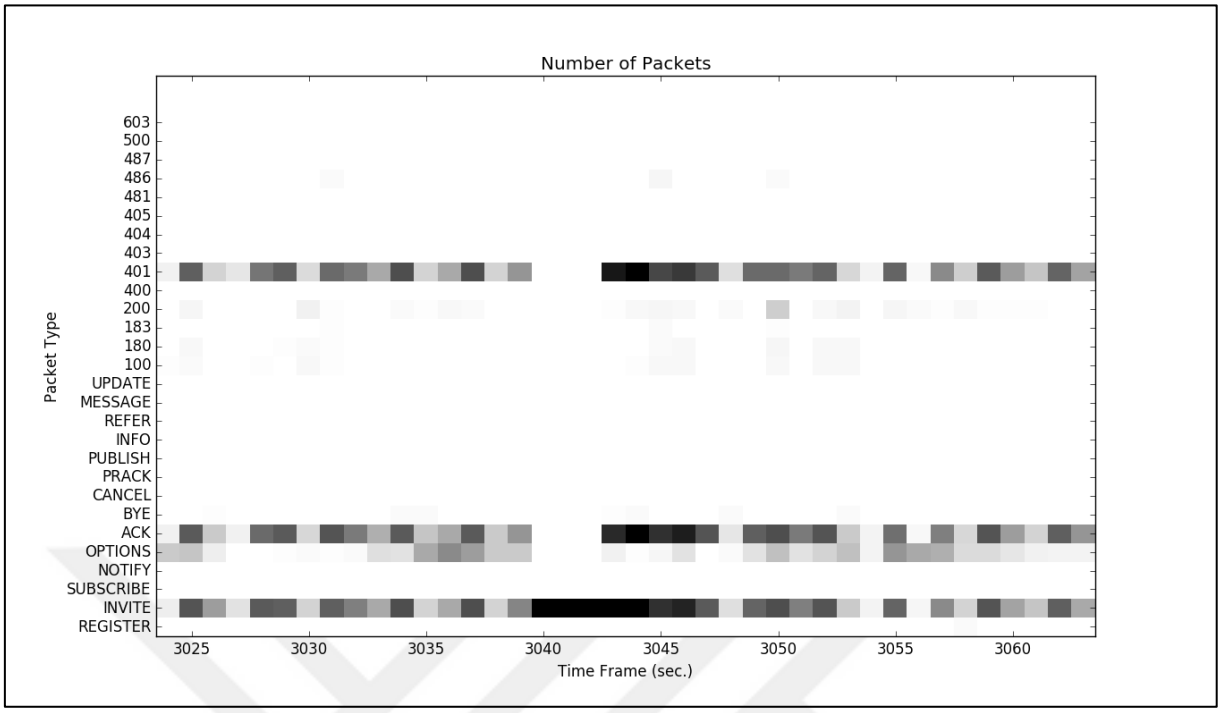
Algoritma	**Başarı Düzeyi**	
NB	Doğruluk:	%98.9286
	Hassasiyet (Precision):	0.964
	Kesinlik (Recall):	1.000
	F-Skoru:	0.982
MLP	Doğruluk:	%99.6429
	Hassasiyet (Precision):	0.988
	Kesinlik (Recall):	1.000
	F-Skoru:	0.994



Şekil 4.5: 50 x INVITE mesajı ile ısı haritası.

Tablo 4.4: 50 INVITE paketi yük yoğunluğuna bağlı başarı değerleri.

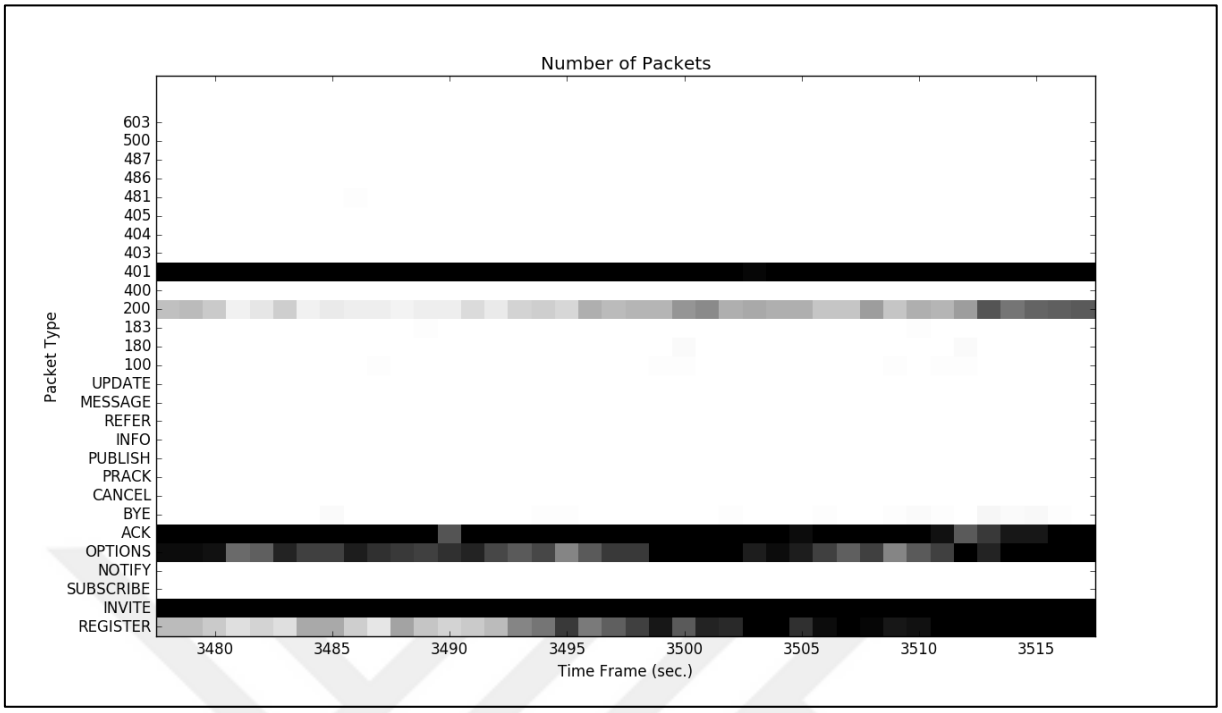
Algoritma	**Başarı Düzeyi**	
NB	Doğruluk:	%99.7619
	Hassasiyet (Precision):	0.992
	Kesinlik (Recall):	1.000
	F-Skoru:	0.996
MLP	Doğruluk:	%100
	Hassasiyet (Precision):	1.000
	Kesinlik (Recall):	1.000
	F-Skoru:	1.000



Şekil 4.6: 100 x INVITE mesajı ile ısı haritası.

Tablo 4.5: 100 INVITE paketi yük yoğunluğuna bağlı başarı değerleri.

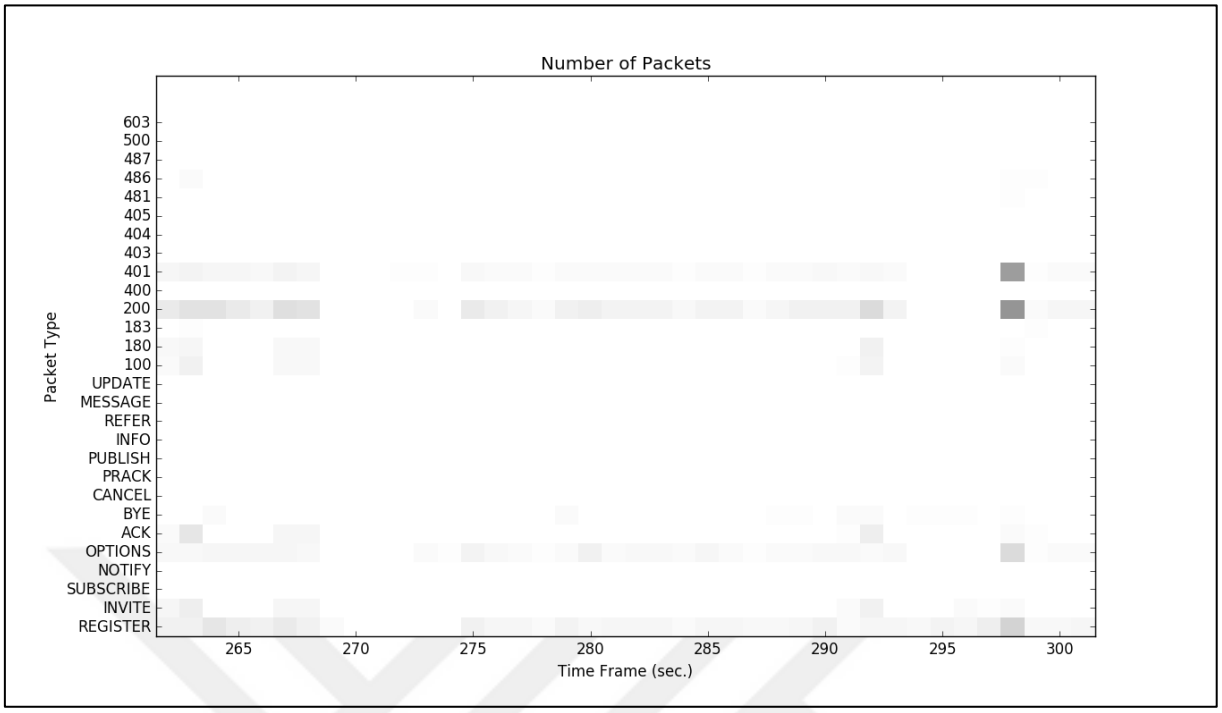
Algoritma	**Başarı Düzeyi**	
NB	Doğruluk:	%99.1667
	Hassasiyet (Precision):	0.972
	Kesinlik (Recall):	1.000
	F-Skoru:	0.986
MLP	Doğruluk:	%99.881
	Hassasiyet (Precision):	1.000
	Kesinlik (Recall):	0.996
	F-Skoru:	0.998



Şekil 4.7: 500 x INVITE mesajı ile ısı haritası.

Tablo 4.6: 500 INVITE paketi yük yoğunluğuna bağlı başarı değerleri.

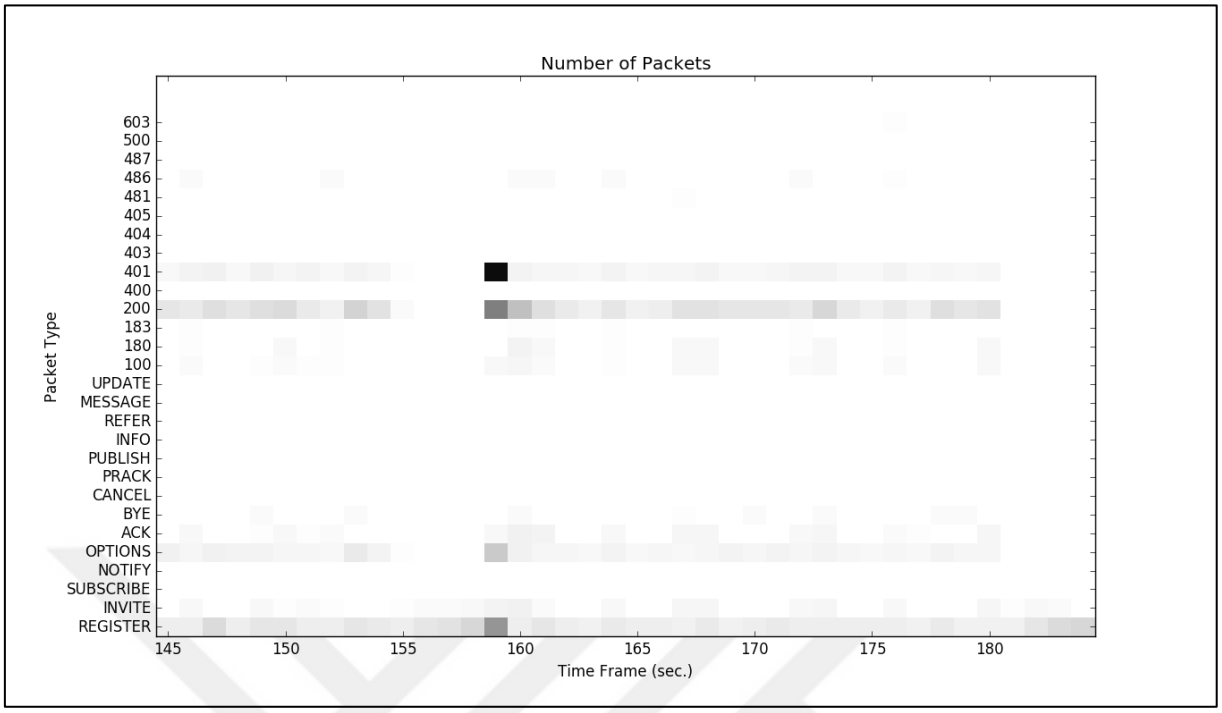
Algoritma	**Başarı Düzeyi**	
NB	Doğruluk:	%99.6429
	Hassasiyet (Precision):	0.988
	Kesinlik (Recall):	1.000
	F-Skoru:	0.994
MLP	Doğruluk:	%99.7619
	Hassasiyet (Precision):	1.000
	Kesinlik (Recall):	0.992
	F-Skoru:	0.996



Şekil 4.8: 5 x REGISTER mesajı ile ısı haritası.

Tablo 4.7: 5 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri.

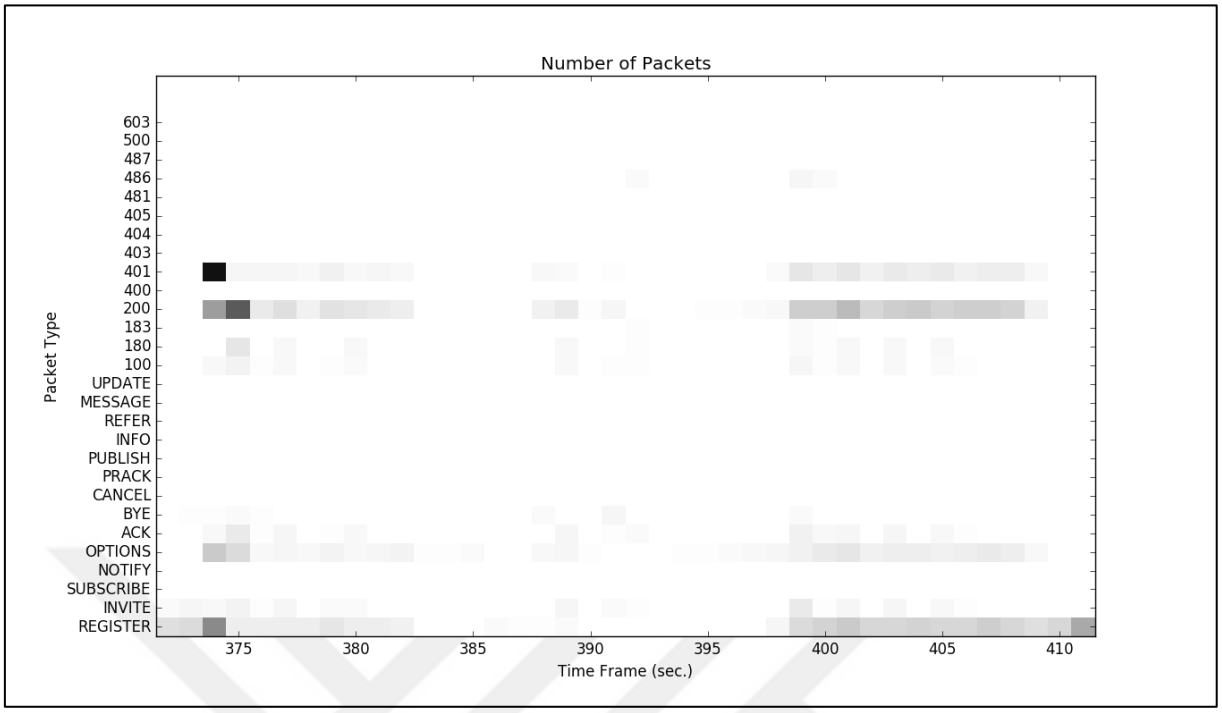
Algoritma	**Başarı Düzeyi**	
NB	Doğruluk:	%96.9048
	Hassasiyet (Precision):	0.973
	Kesinlik (Recall):	0.917
	F-Skoru:	0.944
MLP	Doğruluk:	%97.2619
	Hassasiyet (Precision):	0.954
	Kesinlik (Recall):	0.950
	F-Skoru:	0.952



Şekil 4.9: 10 x REGISTER mesajı ile ısı haritası.

Tablo 4.8: 10 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri.

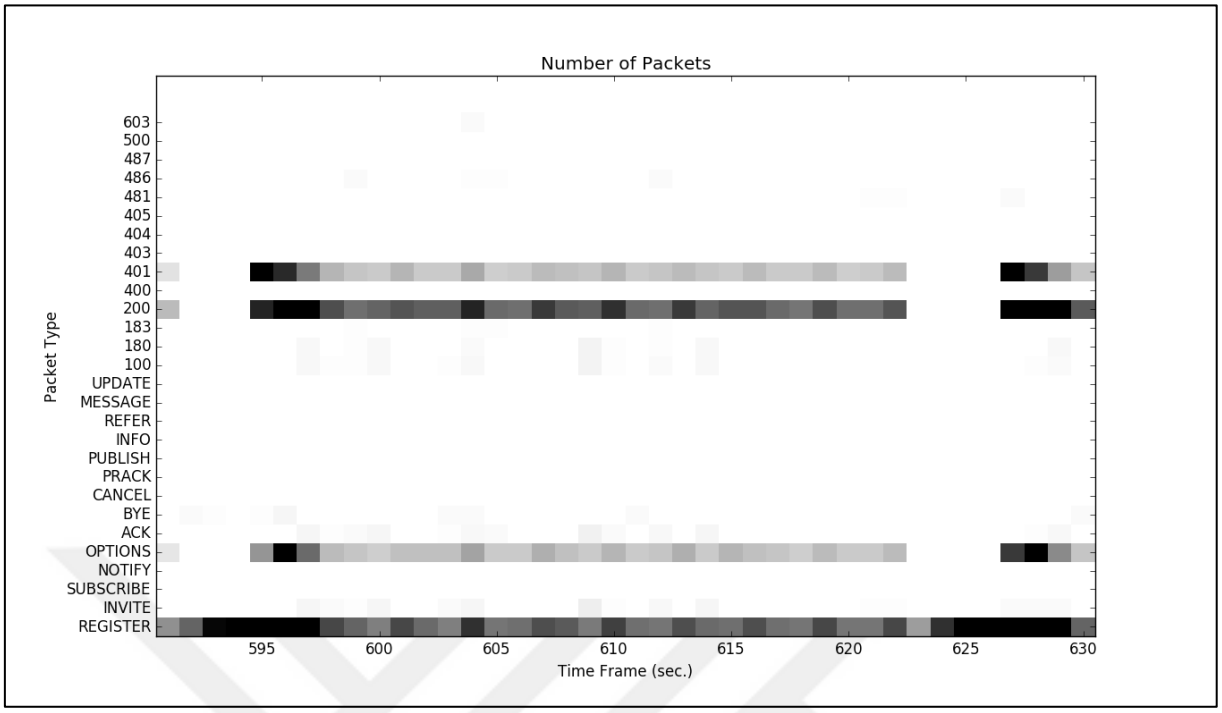
Algoritma	**Başarı Düzeyi**	
NB	Doğruluk:	%99.7619
	Hassasiyet (Precision):	0.992
	Kesinlik (Recall):	1.000
	F-Skoru:	0.996
MLP	Doğruluk:	%99.881
	Hassasiyet (Precision):	0.996
	Kesinlik (Recall):	1.000
	F-Skoru:	0.998



Şekil 4.10: 20 x REGISTER mesajı ile ısı haritası.

Tablo 4.9: 20 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri.

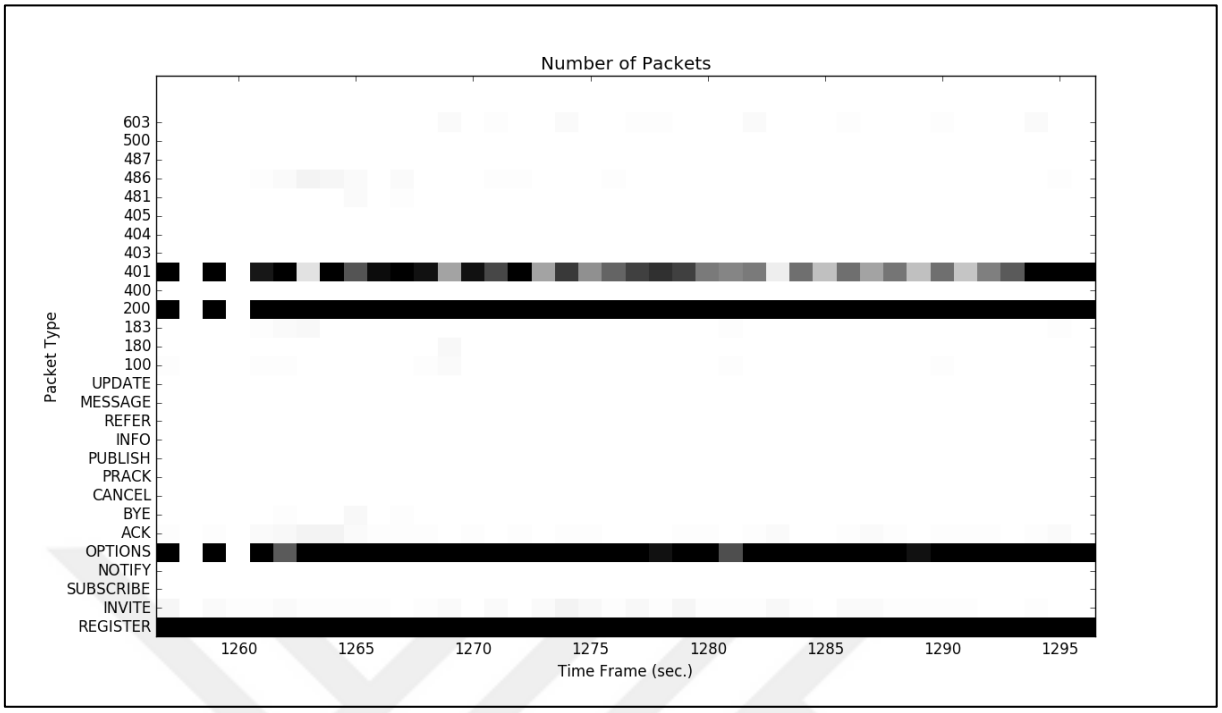
Algoritma	**Başarı Düzeyi**	
NB	Doğruluk:	%99.7619
	Hassasiyet (Precision):	0.992
	Kesinlik (Recall):	1.000
	F-Skoru:	0.996
MLP	Doğruluk:	%99.881
	Hassasiyet (Precision):	0,996
	Kesinlik (Recall):	1.000
	F-Skoru:	0,998



Şekil 4.11: 50 x REGISTER mesajı ile ısı haritası.

Tablo 4.10: 50 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri.

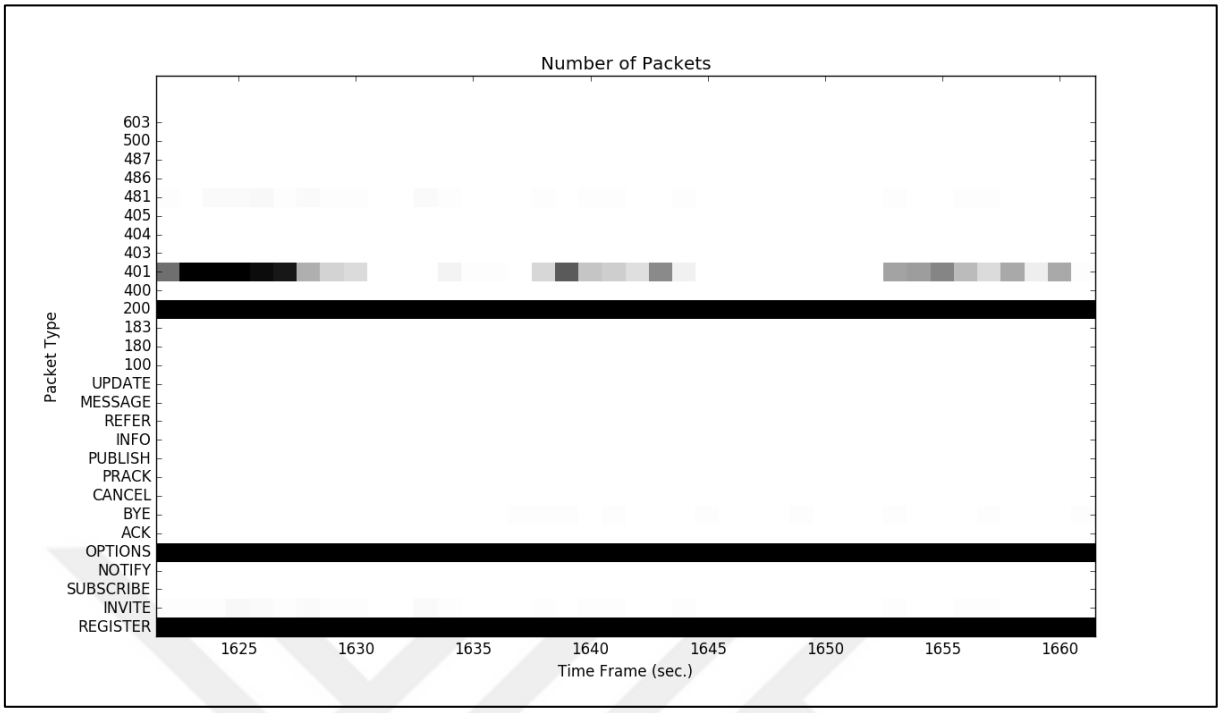
Algoritma	**Başarı Düzeyi**	
NB	Doğruluk:	%100
	Hassasiyet (Precision):	1.000
	Kesinlik (Recall):	1.000
	F-Skoru:	1.000
MLP	Doğruluk:	%100
	Hassasiyet (Precision):	1.000
	Kesinlik (Recall):	1.000
	F-Skoru:	1.000



Şekil 4.12: 100 x REGISTER mesajı ile ısı haritası.

Tablo 4.11: 100 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri.

Algoritma	**Başarı Düzeyi**	
Naive Bayes	Doğruluk:	%99.881
	Hassasiyet (Precision):	0.996
	Kesinlik (Recall):	1.000
	F-Skoru:	0.998
ÇKA	Doğruluk:	%100
	Hassasiyet (Precision):	1.000
	Kesinlik (Recall):	1.000
	F-Skoru:	1.000



Şekil 4.13: 500 x REGISTER mesajı ile ısı haritası.

Tablo 4.12: 500 REGISTER paketi yük yoğunluğuna bağlı başarı değerleri.

Algoritma	**Başarı Düzeyi**	
Naive Bayes	Doğruluk:	%99,881
	Hassasiyet (Precision):	0,996
	Kesinlik (Recall):	1.000
	F-Skoru:	0,998
ÇKA	Doğruluk:	%100
	Hassasiyet (Precision):	1.000
	Kesinlik (Recall):	1.000
	F-Skoru:	1.000

İlgili tablolara ait değerlendirmeler Şekil 4.14 ve Şekil 4.17 içeriklerinde özetlenmiştir.

Başarı kriterleri belirlenirken farklı istatistiksel parametreler değerlendirildi.

Burada saldırı sınıfına ait doğruluk (accuracy), hassasiyet (precision), kesinlik (recall) ve ayrıca hassasiyet ve kesinlik değerlerinin harmonik ortalaması olan f skorunu değerlendirdik.

Saldırı sınıfına ait hassasiyeti hesaplamak için

DP = Doğru pozitif

DN = Doğru negatif

YP = Yanlış pozitif

YN = Yanlış negatif

olmak üzere;

$$Hassasiyet = \frac{DP}{DP + YN} \tag{4.1}$$

Kesinliği hesaplamak için

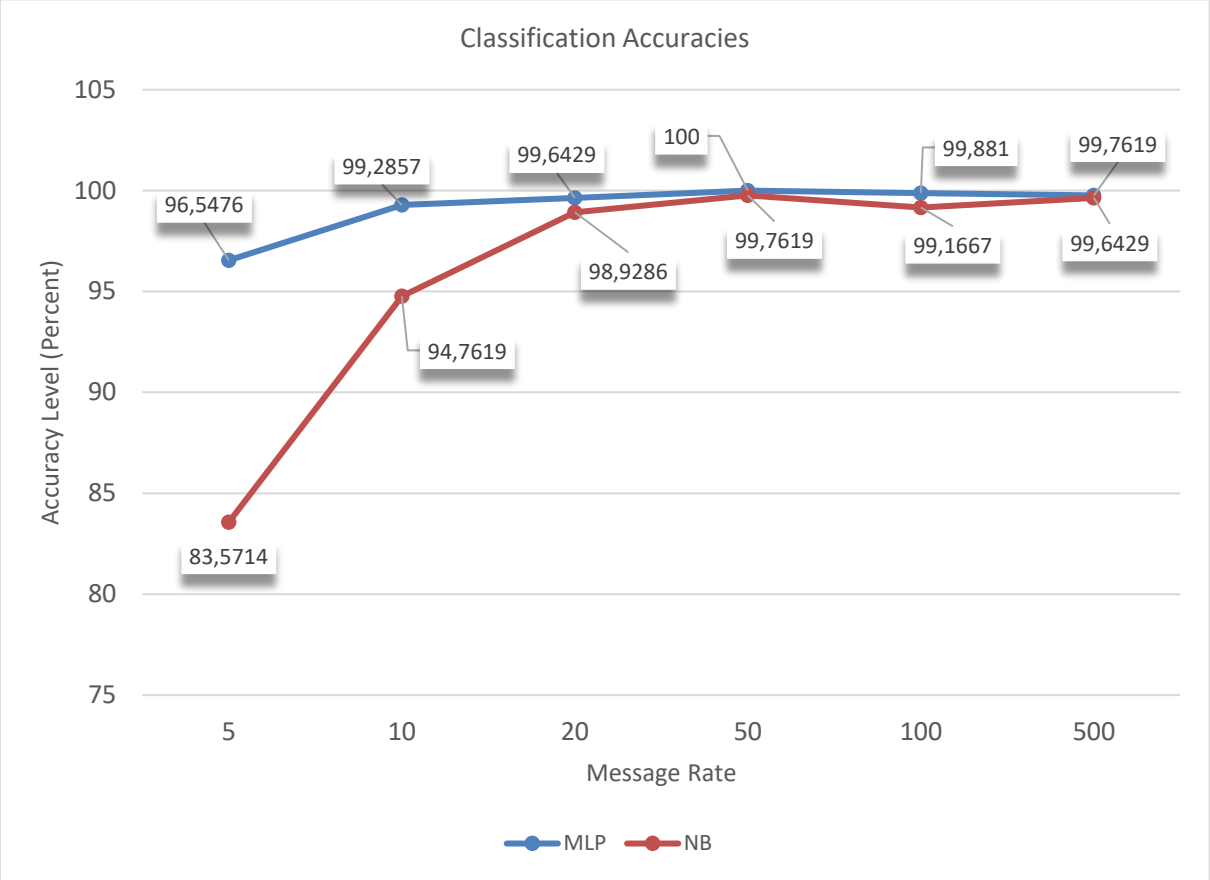
$$Kesinlik = \frac{DP}{DP + YP} \tag{4.2}$$

F skorunu hesaplamak için;

$$F\ skoru = 2 \times \frac{Hassasiyet \times Kesinlik}{Hassasiyet + Kesinlik} \tag{4.3}$$

denklemleri kullanılır.

Toplam örnek içerisinde aradığımız sınıfa ait örnek sayısı çok düşük olduğunda yüzde üzerinden verdiğimiz doğruluk değeri çok yüksek olsa da aslında beklediğimiz başarının sağlanmadığı durumları da ifade ediyor olabilir. Bu durumda f skoru bizim saldırı sınıfını değerlendirmemiz açısından daha anlamlı bir sonuç verecektir.



Şekil 4.14: Farklı INVITE saldırı yüklerine göre algoritmaların doğruluk cinsinden sınıflandırma başarı düzeyleri.

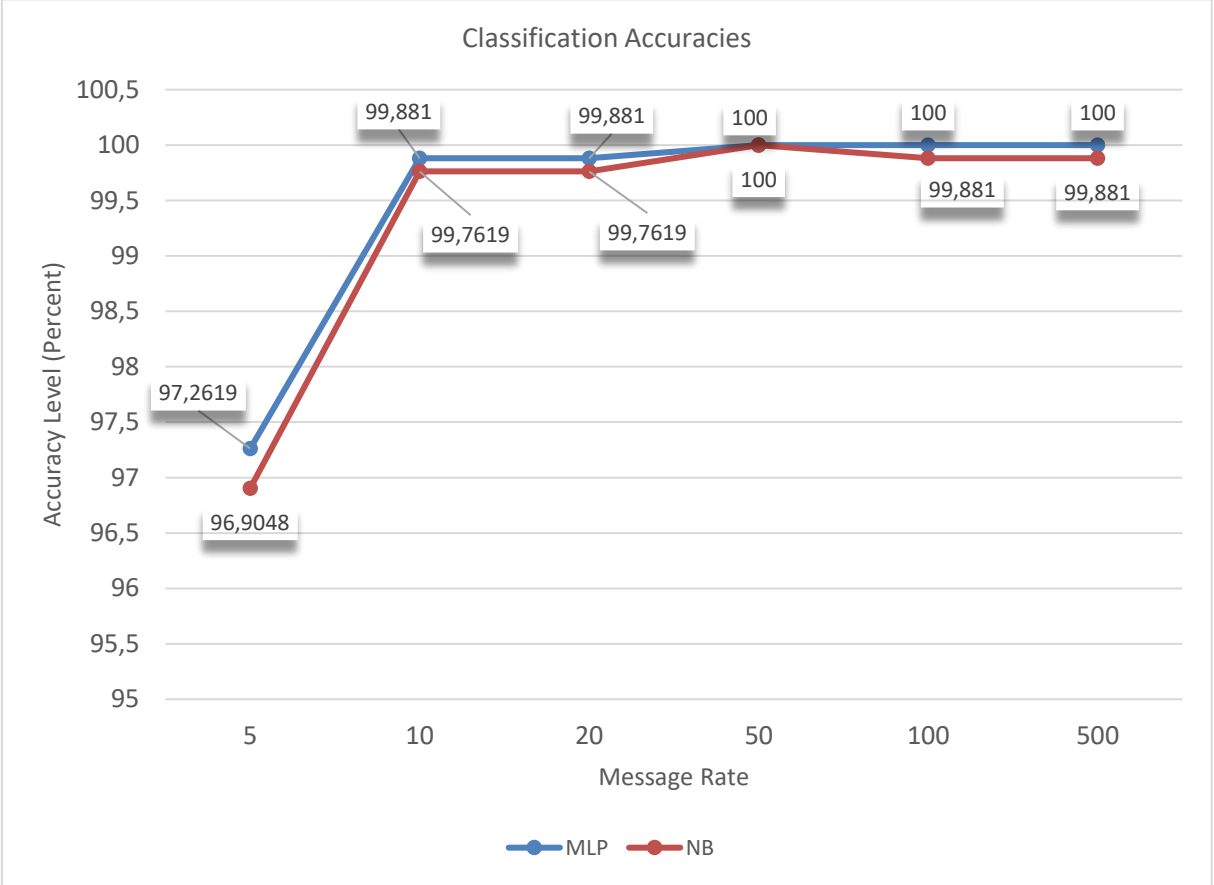
Sınıflandırma başarılarını değerlendirirken Şekil 4.14 ve Şekil 4.17 arasındaki şekillerde çizilen eğrilerde saldırı yoğunluğu artışına bağlı olarak genel bir başarı yükselişi gözlemliyoruz. Şekil 4.14'te saldırı yoğunluğu 50 INVITE paketine yükseldiği zaman başarının MLP algoritması için doğruluğun %100'e çıktığını sonra hafifçe 100 INVITE ve 500 INVITE için düştüğünü gözlemliyoruz. NB algoritmasında ise bu düşüşün biraz daha fazla olduğu görülüyor. Tüm benzetim boyunca normal trafik olarak etiketlediğimiz arka plan trafiği olasılıksal bir dağılımla belirli bir anda minimum 0 çağrı üretme ihtimaline ve 6 adet sanal makinadan 6'şar kullanıcı ile yapılacak benzetim boyunca bir anda toplam olarak maksimum 36 çağrıyı içerme ihtimaline sahiptir. Bu durumda saldırı oranlarını artırdığımızda; yaptığımız benzetimin olasılıksal doğasıyla birlikte başarının büyük ölçüde artma eğilimi, küçük değişimler olsa da tutarlı görülmektedir. Yine grafiklerde ayrıca değerlendirebileceğimiz husus, genel itibariyle MLP algoritmasının tüm saldırı yoğunlukları için NB algoritmasına göre daha başarılı sonular verdiğidir. MLP algoritması tüm saldırı yoğunlukları için %96 üzerinde başarı sağlamıştır.



Şekil 4.15: Farklı INVITE saldırı yüklerine göre algoritmaların f skoru cinsinden sınıflandırma başarı düzeyleri.

Şekil 4.15'te mevcut f skoru değerlerini değerlendirdiğimizde ise MLP algoritmasının yine tüm INVITE saldırı yoğunluğu için maksimum f skoru olan 1 değeri ve yakın değerlere sahip olduğunu görebiliyoruz. NB algoritmasının ise saldırı yoğunluğu 5 paket olduğunda f skoru 0,6 civarı olmakla beraber, daha yoğun saldırılarda 0,9 üzeri f skor değerleriyle MLP algoritmasına saldırı yoğunluğuna bağlı olarak yakınsadığı gözlemlenebiliyor. F skoru değerlerini incelediğimizde yine genel itibariyle tüm saldırı yoğunlukları için INVITE saldırılarında MLP algoritmasının daha yüksek başarıya sahip olduğunu görebiliyoruz.

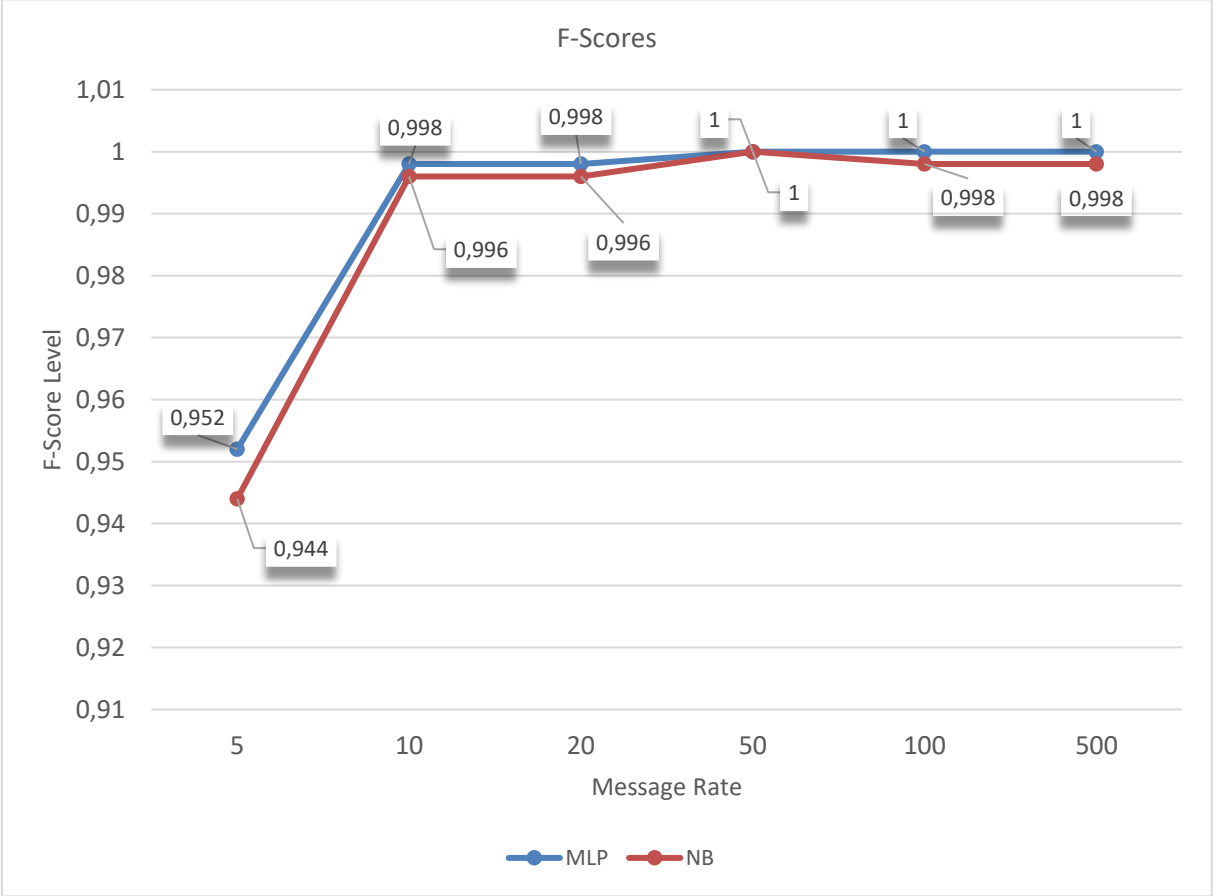
Yine Şekil 4.16 üzerinde REGISTER saldırılarına ait doğruluk değerlerine baktığımızda REGISTER saldırı yoğunluğu 5 olduğunda MLP ve NB algoritmalarının başarı düzeyleri arasında bir miktar fark var iken, REGISTER saldırı yoğunluğu 10 olduktan sonra MLP ve NB algoritmaları arasındaki başarı farkının daha da düştüğünü görüyoruz.



Şekil 4.16: Farklı REGISTER saldırı yüklerine göre algoritmaların doğruluk cinsinden sınıflandırma başarı düzeyleri.

Diğer saldırı yoğunluklarında ise, sadece saldırı yoğunluğu 50 olduğunda her iki algoritmanın aynı doğruluk düzeyinde başarı ürettiğini görebiliyoruz. Daha yüksek saldırı yoğunluklarında ise MLP algoritmasının az da olsa daha yüksek doğruluk düzeyine sahip olduğunu gözlemleyebiliyoruz.

Şekil 4.17 üzerinde REGISTER saldırıları için algoritmaların f skorlarına baktığımızda ise iki algoritmanın f skorları arasındaki farkın gerçekte çok yüksek olmadığını, hemen hemen her iki algoritmanın da benzer başarı düzeyine sahip olmakla beraber MLP algoritmasının daha tercih edilebilir bir başarı eğrisi çizdiğini gözlemliyoruz. Yine REGISTER saldırılarında da, artan saldırı yoğunluğuna bağlı olarak, sınıflandırma başarısının pozitif yönde arttığını gözlemleyebiliyoruz.



Şekil 4.17: Farklı REGISTER saldırı yüklerine göre algoritmaların f skoru cinsinden sınıflandırma başarı düzeyleri.

5. TARTIŞMA VE SONUÇ

Çalışmada, yapılan olağan trafik benzetimi verileri ve saldırı verileri işlenmiş, daha sonra iki farklı kriterde incelenmiştir. Değerler incelendiğinde durum olağan trafik yüküne yaklaştıkça başarı düşmekte, saldırı yoğunluğu arttıkça genel itibariyle sınıflandırma başarısı artmaktadır. Sınıflandırma başarısına ait değerlerin belirli bir eşikten sonra %100'e yaklaştığı görülmektedir. Burada makine öğrenmesi algoritmaları saldırı trafiği ve sağlıklı trafiğin sınıflandırılabilmesi amacıyla, ilgili trafik desenlerinin öğrenilmesi için kullanılmıştır. Makine öğrenmesinin saldırı izleme amaçlı güçlü bir araç olduğu bu çalışmada gösterilmiştir.

Bu çalışmada, özellik kümesi olarak sadece çağrı süreçlerine ait anlık mesaj histogramları kullanılmıştır. Kesinliği daha yüksek sonuçlar elde etmek için farklı düzeydeki protokol paketleri, sistem logları, sistem kaynakları gibi özellik kümeleri ve bu özellik kümelerinin kendi aralarındaki korelasyonlarından da faydalanmak mümkündür.

Çalışmada MLP algoritmasının mevcut parametreleri özellikle düşük yoğunluklu saldırılarda NB algoritmasından daha yüksek başarı ürettiği gösterilmiştir. Mevcut başarı değerleri, makine öğrenmesinin eğiticili bir yöntem olarak güvenlik mekanizmasında değerlendirilmesi açısından anlamlı sonuçlar üretmiştir.

Daha önce Nassar ve diğ. tarafından Opensips PS gibi sunucuların ürettiği iç istatistikler güvenlik amacıyla SVM algoritması aracılığıyla kullanılmıştır [24]. Benzer şekilde, bu iç istatistikler bizim özellik kümemizi zenginleştirmemize yardımcı olabilir ve bu özellik kümelerini de ilerleyen zamanlardaki çalışmalarımız için şu an kullandığımız algoritmalarla değerlendirebiliriz.

Ayrıca mevcut çalışmayı, farklı parametreler ve derin öğrenme yöntemleri gibi farklı algoritmalarla da test ederek başarı düzeylerini değerlendirebiliriz. İlerleyen süreçte, gerçek kullanıcı davranışını modelleyebilmek için operatörlerden destek alarak anonimleştirilmiş gerçek veri kullanmak çalışmayı gerçek senaryolara daha fazla yaklaştırmak açısından faydalı olacaktır.

VMON süreçleri çerçevesinde çalışma değerlendirildiğinde, ilgili algoritmaların; farklı saldırı desenleri, farklı güvenlik süreçleri ve servis kalitesi için de ayrıca değerlendirilmesi anlamlı olacaktır.

KAYNAKLAR

[1]. Mohr, C., 2014, Report: Global VoIP Services Market to Reach $137 Billion by 2020, http://technews.tmcnet.com/channels/hosted-softswitch/articles/393593-report-global-voip-services-market-reach-137-billion.htm, [Ziyaret Tarihi: 20 Mayıs 2019].

[2]. Rebahi, Y., Nassar, M., Magedanz, T. ve Festor, O., 2011, A survey on fraud and service misuse in voice over IP (VoIP) networks, Information Security Technical Report, 16, 12-19.

[3]. Banerjee, K., 2018, A Brief History of SIP, http://www.siptutorial.net/SIP/background.html [Erişim: 20-May-2019].

[4]. Rosenberg, J., Schulzrinne, H., Columbia, U., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. ve Schooler, E., 2002, SIP: Session Initiation Protocol, https://www.ietf.org/rfc/rfc3261.txt, [Ziyaret tarihi: 20 Mayıs 2019]

[5]. Goncalves, F. E., 2010, Building Telephony Systems with OpenSIPS 1.6, Packt Publishing Ltd, Birmingham, ISBN: 978-1-849510-74-5

[6]. Swale, R. ve Collins.D., 2013, Carrier Grade Voice Over IP, McGraw-Hill, ISBN: 978-0-07-182660-0

[7]. Understanding SIP Messages, 2008, https://www.cisco.com/c/en/us/support/docs/unified-communications/spa3102-voice-gateway-router/108729-pqa-108729.html [Ziyaret tarihi: 20 Mayıs 2019]

[8]. SIP Basic Call Flow, https://www.tutorialspoint.com/session_initiation_protocol/session_initiation_protocol_basic_call_flow.htm, [Ziyaret tarihi: 20 Mayıs 2019]

[9]. Ransome, J. F. ve Rittinghouse J. R., 2005, VoIP Security, Elsevier Digital Press, Burlington, ISBN: 1-55558-332-6

[10]. Keromytis, A. D., 2009, A Survey of Voice over IP Security Research, Information Systems Security: 5th International Conference, Kolkata, India

[11]. VoIP Security Aliance, 2005, VoIP Security and Privacy Threat Taxonomy, http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf, [Ziyaret tarihi: 20 Mayıs 2019]

[12]. Reynolds, B. ve Ghosal, D., 2003, Secure IP Telephony using Multi-layered Protection, Network and Distributed System Security Symposium, San Diego, USA

[13]. Wu, Y. S., Bagchi, S., Garg, S., Singh, N., Tsai, T., 2004, SCIDIVE: A stateful and cross protocol intrusion detection architecture for voice-over-IP environments, International Conference on Dependable Systems and Networks, Florence, Italy

[14]. Geneiatakis, D., Kambourakis, G., Dagiuklas, T., Lambrinoudakis, C. ve Gritzalis, S.,

2005, A framework for detecting malformed messages in SIP networks, 14th IEEE Work. Local Metrop. Area Networks, Crete, Greece

[15]. Chen, E. Y., 2006, Detecting DoS attacks on SIP systems, 1st IEEE Workshop on VoIP Management and Security, Vancouver, Canada

[16]. Niccolini, S., Garroppo, R. G., Giordano, S., Risi, G. ve Ventura, S., 2006, SIP intrusion detection and prevention: recommendations and prototype implementation, 1st IEEE Workshop on VoIP Management and Security, Vancouver, Canada

[17]. Sengar, H., Wangh, H., Wijesekera, D. ve Jajodia, S., 2006, Fast detection of denial-of-service attacks on IP telephony, 14th International Workshop on Quality of Service, New Haven, USA

[18]. Sengar, H., Wijesekera, D., Wang, H. ve Jajodia, S., 2006, VoIP intrusion detection through interacting protocol state machines, International Conference on Dependable Systems and Networks, Philadelphia, USA

[19]. Nassar, M., State, R. ve Festor O., 2006, Intrusion detection mechanisms for VoIP applications, Third annual VoIP security workshop, Berlin, Germany

[20]. Rebahi, Y. ve Sisalem, D., 2007, Change-point detection for voice over ip denial of service attacks, Communication in Distributed Systems - 15. ITG/GI Symposium, Bern, Switzerland

[21]. Nassar, M., State, R. ve Festor, O., 2007, VoIP Honeypot Architecture, 10th IFIP/IEEE International Symposium on Integrated Network Management, Munich, Germany

[22]. Bouzida, Y. ve Mangin, C., 2008, A framework for detecting anomalies in VoIP networks, Third International Conference on Availability, Reliability and Security, Barcelona, Spain

[23]. Rieck, K., Wahl, S., Laskov, P., Domschitz, P. ve Müller, K. R., 2008, A self-learning system for detection of anomalous SIP messages, International Conference on Principles, Systems and Applications of IP Telecommunications, Heidelberg, Germany

[24]. Ehlert, S., Wang, C., Magedanz, T. ve Sisalem, D, 2008, Specification-based denial-of-service detection for SIP voice-over-IP networks, The Third International Conference on Internet Monitoring and Protection, Bucharest, Romania

[25]. Tang, J., Cheng, Y. ve Zhou, C, 2009, Sketch-based SIP flooding detection using Hellinger distance, IEEE Global Telecommunications Conference, Honolulu, USA

[26]. Nassar, M., State, R. ve Festor, O., 2010, A framework for monitoring SIP enterprise networks, Fourth International Conference on Network and System Security, Melbourne, Australia

[27]. Aziz, S. ve Gul, M., 2010, A self learning model for detecting SIP malformed message attacks, 3rd IEEE International Conference on Broadband Network and Multimedia Technology, Beijing, China

[28]. Nassar, M., State, R. ve Festor O., 2010, Labeled VoIP data-set for intrusion detection evaluation, 16th EUNICE/IFIP WG 6.6 Workshop, Trondheim, Norway

[29]. Nassar, M., Dabbebi, O., Badonnel, R. ve Festor, O., 2010, Risk management in VoIP infrastructures using support vector machines, International Conference on Network and Service Management, Niagara Falls, Canada

[30]. Ferdous, R., Lo Cigno, R. ve Zorat, A., 2012, Classification of SIP Messages by a Syntax Filter and SVMs, IEEE Global Communications Conference, Anaheim, USA

[31]. Fakis, A., Kambourakis, G., Kolias, C., Papamartzivanos, D., Tsiatsikas, Z. Ve Geneiatakis, D., 2015, Battling Against DDoS in SIP - Is Machine Learning-based Detection an Effective Weapon?, 12th International Joint Conference on e-Business and Telecommunications, Colmar, France

[32]. Tas, I. M., Uğurdogan, B. ve Baktir, S., 2016, Novel session initiation protocol-based distributed denial-of-service attacks and effective defense strategies, Computers & Security, 63, 29-44

[33]. Yıldız, Ç., Kurt, B., Ceritli, T. Y., Sankur, B. ve Cemgil, A. T., 2018, A real-time SIP network simulation and monitoring system, SoftwareX, 8, 21-25

[34]. Kurt, B., Yıldız, Ç., Ceritli, T. Y., Sankur, B. ve Cemgil, A. T., 2018, A Bayesian change point model for detecting SIP-based DDoS attacks, Digital Signal Processing, 77, 48-52

[35]. Chi, S. ve Womack, B. F., 2009, Predicting the Quality of Voice over IP Networks, 2009 IEEE International Workshop Technical Committee on Communications Quality and Reliability, 1-4

[36]. Radhakrishnan, K. ve Larijani, H., 2010, A Study on QoS of VoIP networks: A Random Neural Network (RNN) Approach, Spring Simulation Multiconference 2010, Orlando, USA

[37]. Larijani, H. ve Radhakrishnan, K, 2010, Voice Quality in VoIP Networks Based on Random Neural Networks, 9th International Conference on Networks, French Alps, France

[38]. Öztemel, E., 2012, Yapay Sinir Ağları, Papatya Yayıncılık, İstanbul, ISBN: 978-975-6797-39-6

[39]. Özkan, Y., 2008, Veri Madenciliği Yöntemleri, Papatya Yayıncılık, İstanbul, ISBN: 978-975-6797-82-2

[40]. Yıldız, Ç., BOUN-SIM, https://github.com/cagatayyildiz/boun-sim, [Ziyaret Tarihi: 20-May-2019]

[41]. Trixbox, https://www.voip-info.org/trixbox/, [Ziyaret Tarihi: 20-May-2019]

[42]. Machine Learning at Waikato University, https://www.cs.waikato.ac.nz/ml/index.html, [Ziyaret Tarihi: 20-May-2019]

[43]. Free Angular Admin Template, https://coreui.io/angular/, [Ziyaret Tarihi: 10-May-2019]

[44]. Emara, T., How to use Weka in your Java code, http://www.emaraic.com/blog/weka-java-example, [Ziyaret Tarihi: 10-May-2019]

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Sabit ÇAKIR
Doğum Yeri	Üsküdar
Doğum Tarihi	06.05.1984
Uyruğu	☑ T.C. ❒ Diğer:
Telefon	
E-Posta Adresi	sabit.c@ogr.iu.edu.tr
Web Adresi	

Eğitim Bilgileri	
Lisans	
Üniversite	Maltepe Üniversitesi
Fakülte	Mühendislik ve Doğa Bilimleri
Bölümü	Bilgisayar Mühendisliği
Mezuniyet Yılı	2012

Yüksek Lisans	
Üniversite	İstanbul Üniversitesi-Cerrahpaşa
Enstitü Adı	Lisansüstü Eğitim Enstitüsü
Anabilim Dalı	Bilgisayar Mühendisliği Anabilim Dalı
Programı	Bilgisayar Mühendisliği Programı

Makale ve Bildiriler