DÜZCE ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

VİDEO KONFERANS UYGULAMALARINDA GÜVENLİK DUVARI VE SANAL ÖZEL AĞ (VPN) KULLANIMININ FARKLI AĞLARDA PERFORMANS ANALİZİ

SERDAR ARPACI

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMAN
DOÇ. DR. ARAFAT ŞENTÜRK

DÜZCE, 2024

T.C.
DÜZCE ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

VİDEO KONFERANS UYGULAMALARINDA GÜVENLİK DUVARI VE SANAL ÖZEL AĞ (VPN) KULLANIMININ FARKLI AĞLARDA PERFORMANS ANALİZİ

Serdar ARPACI tarafından hazırlanan tez çalışması aşağıdaki jüri tarafından Düzce Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Doç. Dr. Arafat ŞENTÜRK

Düzce Üniversitesi

Jüri Üyeleri

Doç. Dr. Arafat ŞENTÜRK
Düzce Üniversitesi _____

Doç. Dr. Mehmet ŞİMŞEK
Düzce Üniversitesi _____

Doç. Dr. Muhammed Enes BAYRAKDAR
Milli Savunma Üniversitesi _____

Tez Savunma Tarihi: 05/06/2024

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

5 Haziran 2024

Serdar ARPACI

TEŞEKKÜR

Yüksek lisans öğrenimimde ve bu tezin hazırlanmasında gösterdiği her türlü destek ve yardımdan dolayı çok değerli hocam Doç. Dr. Arafat ŞENTÜRK'e en içten dileklerimle teşekkür ederim.

Bu çalışma boyunca yardımlarını ve desteklerini esirgemeyen sevgili aileme ve değerli çalışma arkadaşlarıma sonsuz teşekkürlerimi sunarım.

5 Haziran 2024 **Serdar ARPACI**

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

ÇİZELGE LİSTESİ

Sayfa No

KISALTMALAR

AP	Access Point
API	Application Programming Interface
DiffServ	Differentiated Services
DSR	Dynamic Source Routing
FIFO	First-In-First-Out
FPS	Frames Per Second
FTP	File Transfer Protocol
HTTP	Hyper-Text Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
L2TP	Layer 2 Tunneling Protokol
LAN	Local Area Network
MAC	Media Access Control
Mbps	Megabits Per Second
MPLS	Multiprotocol Label Switching
NS-2	Network Simulator-2
NS-3	Network Simulator-3
OMNeT++	Objective Modular Network Testbed
OPNET	OPtimized Network Engineering Tool
OTcl	Object-oriented Tool Command Language
PQ	Priority Queuing
Tcl	Tool Command Language
VCR	Video Cassette Recorder
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WFQ	Weighted-Fair Queuing
WLAN	Wireless Local Area Network

ÖZET

VİDEO KONFERANS UYGULAMALARINDA GÜVENLİK DUVARI VE SANAL ÖZEL AĞ (VPN) KULLANIMININ FARKLI AĞLARDA PERFORMANS ANALİZİ

Serdar ARPACI

Düzce Üniversitesi
Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı
Yüksek Lisans Tezi
Danışman: Doç. Dr. Arafat ŞENTÜRK

Haziran 2024, 51 sayfa

Bilgi ve iletişim teknolojilerindeki gelişmeler ve internet kullanım maliyetlerinin düşmesi; e-devlet, e-ticaret, e-sağlık, e-öğrenme gibi uygulama alanlarıyla bu teknolojileri hayatımızın her alanının vazgeçilmez öğesi haline getirmiştir. Özellikle küresel Covid-19 salgın süreci; altyapısını video konferans teknolojisinin oluşturduğu e-öğrenme ve e-toplantı gibi uygulama alanlarında zorunlu gelişmelere neden olmuştur. Video konferans, aynı anda farklı yerlerde bulunan kişilerin, belirli uygulamalar ve internet bağlantısı kullanarak görüntülü ve sesli bir şekilde iletişim kurmalarını sağlar. Video konferans teknolojisinde; arama yapan ve aramayı cevaplayan kişiler arasında gerçek zamanlı, çift yönlü ve büyük boyutlu bir veri akışı olmaktadır. İnternet üzerinden sunulan uygulamaların hızla yaygınlaşmasına sebep olan teknolojideki gelişmeler, aynı zamanda internete bağlı cihaz sayısında ve internet üzerinden akan veri trafiğinde çok ciddi artışlara sebep olmaktadır. Bunun neticesi olarak, video konferans uygulamaları gibi internet üzerinden kullanılan uygulamaların güvenlik ihtiyaçları da artan güvenlik tehdidi riskleriyle orantılı olarak artmaktadır. Güvenlik duvarı ve sanal özel ağ kullanımı, internet üzerinden kullanılan uygulamalar için en temel güvenlik çözümlerindendir. Güvenlik duvarı, kurumsal bir ağ ile internet bulutu arasına konumlandırılarak ağa gelen ve giden trafiği tanımlı kurallara göre filtreleyen cihazdır. Bu yönüyle güvenlik duvarı, kurallara uyan ağ trafiğine izin veren, kurallara uymayan ağ trafiğini ise engelleyen bir rol üstlenir. Sanal özel ağ ise, kurumsal bir ağa, internet bulutu üzerinden noktadan noktaya güvenli bir bağlantı sağlar. Bu işlemi yaparken iki uç düğüm arasındaki veri iletişimini IP (İnternet Protokolü) tüneli adı verilen sanal bağlantılar kullanarak gerçekleştirir. Bu çalışmada, video konferans uygulamalarının farklı ağlarda güvenlik duvarı ve sanal özel ağ ile kullanımının uygulama performansına etkileri analiz edilmiştir. Bu etkilerin analizinin yapılması ağ protokollerinde, ağ bileşenlerinde ve video konferans uygulamalarında daha sonra yapılabilecek iyileştirmeler için yol gösterici olacaktır. Benzetim metodunun kullanıldığı bu çalışmada, OPNET benzetim aracı ile oluşturulan farklı senaryoların benzetimiyle elde edilen veriler karşılaştırılmalı olarak analiz edilmiştir.

Anahtar Sözcükler: Ağ Performansı, Güvenlik Duvarı, OPNET, Sanal Özel Ağ (VPN), Video Konferans

ABSTRACT

PERFORMANCE ANALYSIS OF VIDEO CONFERENCING APPLICATIONS WITH USE OF FIREWALL AND VIRTUAL PRIVATE NETWORK (VPN) IN DIFFERENT NETWORKS

Serdar ARPACI
Düzce University
Graduate School, Department of Computer Engineering
Master's Thesis
Supervisor: Assoc. Prof. Dr. Arafat ŞENTÜRK

June 2024, 51 pages

The developments in information technologies have made these technologies indispensable elements of our lives with application areas such as e-government, e-commerce, e-health, e-learning. Particularly the global Covid-19 pandemic period has led to forced developments in e-learning and e-meeting application areas, the infrastructure of which is formed by video conferencing technology. Video conferencing allows users who are simultaneously in different locations to communicate via video and audio over the internet using specific applications. In video conferencing technology, there is a real-time, bidirectional, and large-scale data flow between the calling and called users. Developments in technology, which cause the rapid increase of applications served over internet, also cause a significant increase in the number of devices connected to internet and the data traffic flowing over internet. As a result, the security needs of applications used over internet, such as video conferencing applications, are increasing in proportion to the increasing security threat risks. The use of firewall and VPN (Virtual Private Network) are the most basic security solutions for applications used over internet. A firewall is a device, which is positioned between a corporate network and the internet cloud, filtering incoming and outgoing traffic to and from the network according to defined rules. Thus, the firewall plays the role of allowing traffic that complies with the rules and blocking traffic that does not. VPN, on the other hand, provides a secure point-to-point connection to a corporate network through the internet cloud. While doing this process, it provides data communication between the two end nodes using virtual connections called IP (Internet Protocol) tunnels. This study analyses the effects of using video conferencing applications with firewall and VPN in different networks on application performance. Analysis of these effects will be the basis for future improvements in network protocols, network components and video conferencing applications. In the study in which the simulation method was used, the data obtained from the simulation of different scenarios created with OPNET tool were analyzed comparatively.

Keywords: Firewall, Network Performance, OPNET, Video Conferencing, VPN

1. GİRİŞ

Bu bölümde, ilk olarak video konferans teknolojisinin gelişimi ve video konferans görüşmelerinin genel özelliklerinden bahsedilmiştir. Daha sonra çalışmada hedeflenen amaç ve tezin organizasyonu hakkında bilgi verilmiştir.

1.1. VİDEO KONFERANS TEKNOLOJİSİNİN GELİŞİMİ

Bilgi ve iletişim teknolojilerindeki gelişmeler ile internet kullanım maliyetlerinin düşmesi, bu teknolojileri kullanarak gerçekleştirilen işlem ve süreçlerin gittikçe yaygınlaşmasına sebep olmuştur. Bu süreçte; bilgi ve kaynaklara hızlı ve kolay erişim imkânları doğmuş, iş ve karar alma süreçleri internet üzerinden sağlanan servis ve uygulamalar ile gerçekleştirilebilir hale gelmiş, kurum ve işletmelerin vatandaşlara internet üzerinden sunduğu birçok uygulama ortaya çıkmıştır. Çalışanlar için uzaktan çalışma imkânları doğmuş, kurum ve işletmelerin coğrafi sınırların aşılmasıyla esnek çalışma modellerine geçişi sağlanmıştır [1], [2]. Eğitim kurumlarında uzaktan ve çevrimiçi eğitim uygulamaları ile öğrenme imkânları genişletilmiştir [3], [4]. Özellikle küresel Covid-19 salgın süreci; altyapısını video konferans teknolojisinin oluşturduğu e-öğrenme ve e-toplantı gibi uygulama alanlarında zorunlu gelişmelere neden olmuştur [4], [5], [6], [7], [8].

Video konferans, aynı anda farklı yerlerde bulunan kişilerin internet bağlantısı üzerinden birbirleriyle sesli ve görüntülü olarak iletişim kurabilmesini sağlayan bir iletişim teknolojisidir [9], [10]. Bu teknoloji, katılımcıların sesli konuşma, görüntülü görüşme ve ekran paylaşımı gibi çeşitli özellikleri kullanarak etkileşimde bulunmalarına olanak sağlar [11], [12]. Video konferans; genellikle iş toplantıları, uzaktan eğitim, uzaktan çalışma ve kişisel görüşmeler gibi amaçlarla kullanılmaktadır [13]. Bu teknoloji, birkaç kişinin katılımıyla oluşan sesli ve görüntülü görüşmelerde kullanılabileceği gibi, onlarca katılımcının bulunduğu sesli ve görüntülü görüşmelerde de kullanılabilir [12].

Günümüzde kullanılan en popüler video konferans uygulamaları; Zoom, Google Meet, Microsoft Teams ve Skype uygulamalarıdır [12], [14]. Bu uygulamaların bir kısmı kısıtlı özelliklerle ücretsiz olarak kullanılabilmekte veya lisans satın alınarak tüm özellikler

kullanılabilir olmaktadır. Bazıları açık kaynak kodlu olup tüm özellikleriyle ücretsiz olarak kullanılabilmektedir [15], [16].

1.2. VİDEO KONFERANS GÖRÜŞMELERİNİN ÖZELLİKLERİ

Video konferans görüşmelerinde; görüşme aramasını yapan ve aramayı cevaplayan taraflar arasında gerçek zamanlı ve çift yönlü bir iletişim vardır [17]. Bu iletişimde sürekli ve büyük boyutlu bir veri akışı gerçekleşmektedir. Kaliteli bir video konferans görüşmesi için uçtan uca gecikme ve gecikme varyasyonu değerlerinin en aza indirilmesi, paket kayıplarının önlenmesi gerekmektedir [17], [18], [19]. Uçtan uca gecikme, bir video paketinin kaynakta üretilmesinden hedefin uygulama katmanına varıncaya kadar geçen süreyi ifade eder [17], [20]. Bir video konferans görüşmesinde, katılımcıların doğal bir şekilde etkileşime girebilmesi için uçtan uca gecikmenin insan algısının altında olması gerekir [10], [21]. Bu değer yaklaşık 100 ms.'dir [10], [21]. Ancak, kaliteli bir video görüşmesi için uçtan uca gecikmenin en fazla 150 ms. olabileceği de iddia edilmektedir [17], [22]. Jitter olarak da ifade edilen paket gecikme varyasyonu, iki ardışık paketin uçtan uca gecikmeleri arasındaki en fazla fark olarak tanımlanır [23]. Diğer bir ifadeyle, ardışık paketlerin varış sürelerindeki tutarsızlığı ifade eder. Video konferans uygulamaları gibi gerçek zamanlı uygulamalar, gecikme varyasyonuna karşı oldukça hassastır. Bir video konferans görüşmesinde yüksek gecikme varyasyonu; ses ve görüntünün senkronize olmasını engelleyerek görüşme kalitesini düşürür ve kullanıcı deneyimini azaltır. Gecikme varyasyonu için kabul edilebilir değer en fazla 50 ms.'dir [20]. Video konferans görüşmelerinde paket kayıplarının önlenmesi de son derece hayati bir öneme sahiptir [24]. Bu bağlamda görüşme kalitesinde belirleyici olan paket kayıp oranı değeri en fazla %1 olabilir [22]. Aksi halde görüşme kalitesi fark edilir biçimde düşmektedir [22].

1.3. ÇALIŞMANIN AMACI

İnternet üzerinden sunulan uygulamaların hızla yaygınlaşmasına sebep olan teknolojideki hızlı gelişmeler, internete bağlı cihaz sayısında ve internet üzerinden akan veri trafiğinde çok ciddi artışlara sebep olmaktadır. Bunun neticesi olarak, internet üzerinden kullanılan uygulamaların güvenlik ihtiyaçları da artan güvenlik tehdidi riskleriyle orantılı olarak artmaktadır [25]. Güvenlik duvarı ve VPN (Virtual Private Network) kullanımı, video

konferans uygulamaları gibi internet üzerinden kullanılan uygulamalar için en temel güvenlik çözümlerindendir. Güvenlik duvarı, kurumsal bir ağın internet bağlantı noktasına yerleştirilen ve üzerinden geçen ağ trafiğini tanımlı kurallara göre filtreleyen bir cihazdır [26]. VPN ise, bir kurumsal ağa, ağ dışındaki bir düğümün internet bulutu üzerinden güvenli bir bağlantı kurmasını sağlar [27].

Bu çalışmada, video konferans uygulamalarının farklı ağ teknolojilerinde güvenlik duvarı ve VPN ile kullanımının uygulama performansına etkileri araştırılmıştır. Benzetim yönteminin kullanıldığı çalışmada farklı benzetim senaryolarının çalıştırılmasıyla elde edilen sonuçların karşılaştırılması ve değerlendirilmesi yapılmıştır.

Daha önce yapılan çalışmalarda HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), e-mail, veritabanı, VoIP (Voice over Internet Protocol) ve video konferans gibi uygulamaların performansları birçok açıdan ele alınmış ve değerlendirilmiştir. Fakat video konferans uygulamalarının farklı ağlarda güvenlik duvarı ve VPN ile kullanımının performans analizine dair bir çalışma bulunmamaktadır. Bu çalışmada hem kullanılan farklı ağ teknolojilerinin hem de güvenlik duvarı ve VPN kullanımının video konferans uygulamalarının performansına olan etkileri tespit edilmiş ve karşılaştırmalı olarak analiz edilmiştir. Bu etkilerin tespit edilerek analizinin yapılması ağ protokollerinde, ağ bileşenlerinde ve video konferans uygulamalarında daha sonra yapılabilecek iyileştirmeler için yol gösterici olacaktır.

1.4. TEZ ORGANİZASYONU

Bu tez çalışması aşağıda verilen bölümler şeklinde organize edilmiştir:

1. Bölümde, ilk olarak video konferans teknolojisinin gelişiminden ve video konferans görüşmelerinin özelliklerden bahsedilmiştir. Video konferans görüşmelerinin kalitesinde belirleyici olan en önemli parametreler hakkında bilgi verilerek kaliteli bir video konferans görüşmesi için bu parametrelerin kabul edilebilir değer aralıkları ifade edilmiştir. Sonrasında çalışmanın amacı açıklanmış ve tezin organizasyonu anlatılmıştır.

2. Bölümde ise literatürde yer alan video konferans performans analizi ve ağ performans analizi ile ilgili çalışmalar hakkında bilgi verilmiştir.

3. Bölümde, öncelikle çalışmada kullanılacak ağ benzetim yönteminden bahsedilmiştir. Ağ benzetimi için kullanılan benzetim araçları hakkında kısaca bilgiler verilip bu

çalışmada kullanılan OPNET ağ benzetim aracı üzerinde durulmuştur. Daha sonra bu çalışmada kullanılan video konferans parametrelerinden bahsedilmiştir.

4. Bölümde ise, ilk önce OPNET benzetim aracı ile modellenen senaryolar ve ağ topolojileri hakkında ayrıntılı bilgi verilmiş, ardından benzetimde toplanan istatistik verilerine değinilmiştir. Daha sonra senaryoların benzetiminden elde edilen istatistik verileri grafiksel olarak gösterilmiştir. Son olarak grafiksel verilerin karşılaştırılması ve analizi yapılmıştır.

5. Bölümde sonuçlar video konferans uygulama performansı açısından değerlendirilmiş ve yorumlanmıştır. Sonrasında çalışmanın kısıtlarına değinilmiştir. Ardından bu çalışma ışığında yapılabilecek sonraki çalışmalarla ilgili önerilerde bulunulmuştur.

2. İLGİLİ ÇALIŞMALAR

Bu bölümde ilk olarak video konferans uygulamalarının performansıyla ilgili önceki çalışmalardan bahsedilmiştir. Daha sonra gecikmeye duyarlı bir diğer gerçek zamanlı uygulama olan VoIP uygulamalarının performansıyla ilgili çalışmalar sunulmuştur. Daha sonra ağ performansıyla ilgili diğer çalışmalara değinilmiştir. Bu bölümde sunulan tüm çalışmalarda benzetim yöntemi kullanılmıştır.

L. Das Dhomeja ve arkadaşları tarafından yapılan çalışma [28], 802.11a, 802.11b ve 802.11g standartlarının video konferans uygulamalarında kullanılmasının uygulama performansı açısından etkilerini analiz etmiştir. Benzetim yönteminin kullanıldığı çalışmada her bir standart için farklı bir senaryo oluşturulmuştur. Senaryoların benzetimleri sırasında uçtan uca gecikme süresi, WLAN (Wireless Local Area Network) gecikme süresi, MAC gecikme süresi, gönderilen paket sayısı, alınan paket sayısı, yük ve verim istatistiksel verileri toplanmıştır. Verilerin analizi sonucunda, video konferans uygulamalarının 802.11a standardında en iyi, 802.11b standardında ise en kötü performansı gösterdiği belirtilmiştir.

M. I. Mohamed Abouseda ve arkadaşlarının yaptığı çalışmada [29] FIFO (First-In-First-Out) ve WFQ (Weighted-Fair Queuing) kuyruklama mekanizmalarının video konferans uygulamalarının performansı üzerindeki etkileri analiz edilmiştir. Çalışmada modellenen senaryoların benzetimleri sırasında uçtan uca gecikme süresi, paket gecikme varyasyonu, gönderilen ve alınan paket sayısı gibi veriler toplanmış ve karşılaştırılmıştır. Çalışma sonucunda uygulama performansı açısından her iki kuyruklama mekanizmasının da kabul edilebilir değer aralıklarında sonuçlar sağladığı ancak FIFO mekanizmasının daha iyi performans sunduğu sonucuna ulaşılmıştır.

K. Sharma ve arkadaşlarının yaptığı çalışma [30] 802.11 standardında HTTP, Remote Login, video konferans ve VoIP uygulamalarının kullanımını performans açısından değerlendirmiştir. Modellenen senaryoların benzetimi sırasında gönderilen paket sayısı ve WLAN verim istatistikleri toplanmış ve analiz edilmiştir. HTTP ve Remote Login uygulamalarında düğüm sayısı daha fazla olmasına rağmen veri akışı video konferans ve VoIP uygulamalarına kıyasla daha düşük olmuştur. Çalışma sonucunda, video konferans

ve VoIP uygulamalarının gecikmeye duyarlı ve gerçek zamanlı uygulamalar olması nedeniyle ağda önceliklendirildiği sonucuna varılmıştır.

P. Singh tarafından yapılan çalışmada [31]; HTTP, FTP, e-mail ve video konferans uygulamaları kullanılarak DSR (Dynamic Source Routing) yönlendirme protokolünün farklı trafik yükleri altındaki performansı analiz edilmiştir. Benzetim senaryolarında performans değerlendirme kriteri olarak uçtan uca gecikme süresi ve verim değerleri kullanılmıştır. Benzetim sonuçlarına göre ortalama uçtan uca gecikme süresi video konferans uygulamasında en yüksek, HTTP uygulamasında ise en düşük sonucu vermiştir. Verim açısından değerlendirildiğinde, video konferans uygulaması ile en yüksek HTTP uygulaması ile en düşük değer elde edilmiştir. Çalışma sonunda, genel olarak DSR yönlendirme algoritması ile en iyi performansı HTTP uygulamasının gösterdiği sonucuna ulaşılmıştır.

H. Mohammed ve arkadaşlarının yaptığı çalışma [32] VoIP uygulamalarının güvenlik duvarı ve VPN ile kullanımını uygulama performansı açısından analiz etmiştir. Modellenen senaryoların benzetimi sırasında uçtan uca gecikme süresi, paket gecikme varyasyonu, gönderilen ve alınan paket sayısı değerleri toplanmıştır. Verilerin analiz edilmesiyle çalışmanın sonucunda VoIP uygulamalarında VPN kullanımının güvenlik duvarı kullanımına göre daha iyi sonuçlar verdiği bulunmuştur.

M. K. Hasan tarafından yapılan çalışmada [33] MPLS (Multiprotocol Label Switching) ve IP yönlendirme algoritmalarının performansı HTTP, FTP, VoIP ve video konferans uygulamaları kullanılarak karşılaştırılmıştır. Senaryoların benzetimi sırasında HTTP sayfa yanıt süresi, gönderilen ve alınan veri miktarı, paket gecikme varyasyonu ve IP paket kayıpları gibi veriler toplanmıştır. Çalışma sonucunda MPLS yönlendirmenin IP yönlendirmeye göre daha iyi performans gösterdiği belirtilmiştir.

M. Aamir ve arkadaşları tarafından yapılan çalışmada [34], PQ (Priority Queuing) ve WFQ kuyruklama mekanizmaları kullanılarak FTP, veritabanı, VoIP ve video konferans uygulamalarının performansı karşılaştırılmıştır. Modellenen senaryoların benzetimi sırasında kuyruk gecikme süresi, kuyruk gecikme varyasyonu, uçtan uca gecikme süresi, tampon bellek kullanımı, ortalama verim gibi istatistiksel veriler toplanmıştır. Verilerin değerlendirildiğinde FTP ve veritabanı uygulamaları ile WFQ mekanizmasının PQ mekanizmasına göre daha iyi performans sağladığı bulunmuştur. Ayrıca hem PQ hem de WFQ mekanizmalarında en yüksek gecikme değerleri video konferans uygulamasında

elde edilmiştir. Çalışma sonucunda; video konferans uygulamalarında tampon bellek miktarının artırılmasıyla tampon bellek kullanımının arttığı, kesilen trafiğin ise azaldığı tespit edilmiştir. Ayrıca video konferans uygulamalarında tampon bellek miktarının artırılmasının paket gecikme varyasyonunu azalttığı bulunmuştur.

M. Jacobi ve arkadaşı tarafından yapılan çalışma [35], IPv4 ve IPv6 ağlarında VoIP uygulamalarının DiffServ (Differentiated Services) mekanizması ile kullanımını uygulama performansı açısından değerlendirmiştir. Performans değerlendirme kriterleri olarak uçtan uca gecikme süresi, paket gecikme varyasyonu ve paket kaybı değerleri kullanılmıştır. Modellenen senaryoların benzetimleri sonunda DiffServ kullanımının hem IPv4 hem de IPv6 ağlarında VoIP uygulama performansını önemli ölçüde artırdığı gözlemlenmiştir.

C. Çakir ve arkadaşının yaptığı çalışmada [36] VoIP uygulamalarında güvenlik duvarı ve VLAN (Virtual Local Area Network) kullanımının etkileri incelenmiştir. Benzetim sonuçlarına göre, güvenlik duvarı kullanımıyla ağın dışından gelen yoğun bir saldırı durumunda uygulama erişilebilirliğinin korunmasına rağmen uygulama cevap sürelerinin artmasına bağlı olarak performansın düştüğü bulunmuştur. Çalışmanın sonucunda, iç ağdan gelen tehditlere karşı güvenlik duvarı kullanımının koruma sağlayamadığı fakat VLAN kullanımının sağlayabildiği ifade edilmiştir. Yine sonuçlar VLAN kullanımının sistemin performansına olumlu katkı sağladığını göstermiştir.

S. Çam tarafından yapılan çalışma [37], güvenlik duvarı ve VPN kullanımının ağ performansı üzerindeki etkilerini analiz etmiştir. HTTP, e-mail ve veritabanı uygulamaları için modellenen senaryoların benzetim sonuçları incelendiğinde, güvenlik duvarı kullanımının uygulama yanıt sürelerini artırdığı, ağ kullanımını ve alınan veri miktarını azalttığı görülmüştür. Çalışmaya göre VPN kullanımı, uygulama yanıt sürelerini güvenlik duvarı kullanımına göre daha fazla artırmış, ancak ağ kullanımını ve alınan veri miktarını güvenlik duvarı kullanımına göre daha fazla azaltmıştır.

M.C. Güleryüz'ün yaptığı çalışmada [38] IEEE tarafından geliştirilen 802.11a, 802.11b, 802.11g, 802.11n kablosuz ağ standartlarının performansı HTTP, FTP ve e-mail uygulamalarının kullanılmasıyla değerlendirilmiştir. Modellenen senaryoların benzetimleri gerçekleştirilerek gerekli istatistik verileri toplanmıştır. Çalışma sonunda yapılan genel değerlendirmede, 802.11n standardının en iyi, 802.11b'nin ise en kötü performansa sahip olduğu ifade edilmiştir. Yine çalışma sonuçları, ağdaki trafik

yoğunluğu artıkça 802.11a standardının 802.11b'den daha iyi bir performans sergilediğini göstermiştir.

3. MATERYAL VE YÖNTEM

Bu bölümde ilk olarak ağ benzetim yöntemi ile benzetim araçlarından bahsedilmiş, ardından çalışmada kullanılan ağ benzetim aracı hakkında bilgi verilmiştir. Daha sonra benzetimde kullanılan video konferans parametreleri anlatılmıştır.

3.1. AĞ BENZETİMİ VE BENZETİM ARAÇLARI

Ağ benzetimi; çeşitli konfigürasyonlar altında çalışan gerçek bir ağın davranışını modelleyerek, ağ topolojilerinin tasarımı, uygulanması, optimizasyonu ve performans değerlendirmesinde yaygın olarak kullanılan bir yöntemdir [39]. Bu yöntem sayesinde; ağ parametrelerini ölçmek için yapılacak çalışmalarda; gerçek düğümler, bağlantılar ve cihazlarla gerçek bir test ağı kurma maliyetine ihtiyaç duyulmadan istenilen senaryolar kontrollü ve tekrarlı olarak çalıştırılabilir [39]. Ağ benzetimi için çeşitli araçlar kullanılmaktadır. Bu araçlar ile fiziksel bir ağda yapılması zor veya imkânsız olan karmaşık ağ topolojileri ve trafik modelleri kolayca oluşturulabilir [40]. Örneğin 200 yönlendirici, 100 anahtar ve 200 düğüm içeren gerçek bir ağı oluşturmak son derece zor iken bu ağı benzetim araçlarıyla oluşturmak mümkündür [41]. Bu araçlar; gerçek bir ağ kurmadan önce farklı protokolleri test etme, farklı ağ tasarım seçeneklerini karşılaştırma ve olası sorunları tespit etme imkânı sunar. NS-2, NS-3, OMNeT++ ve OPNET literatürde kabul görmüş en popüler benzetim araçları arasında bulunmaktadır [40], [42], [43].

NS-2, açık kaynak kodlu bir ağ benzetim aracıdır [42], [44]. NS-2, C++ ile oluşturulmuştur ve benzetim ara yüzünü Tcl'nin nesne yönelimli bir türevi olan OTcl aracılığıyla gerçekleştirir [44]. Ağ topolojisi OTcl komutları ile tanımlanır ve belirlenen parametrelerle NS-2 tarafından benzetimi gerçekleştirilir [44]. NS-2 hem kablolu hem de kablosuz ağların benzetiminde kullanılır [42], [45]. Kullanıcı dostu olmayan metin tabanlı bir arayüz sunması ve benzetim sonuçlarının grafiksel gösterimini sağlamaması NS-2'nun öğrenilmesini ve kullanılmasını zorlaştırmaktadır [43]. Açık kaynak kodlu olması nedeniyle kısıtlı bir dokümantasyona sahip olması, iyi bir senaryo için araç eksikliği ve kullanıcı kodundaki güncellemelerin yeniden derlenmeyi gerektirmesi NS-2'nin

dezavantajları olarak sayılabilir [42].

NS-3, birçok ağ topolojisini ve protokolünü destekleyen açık kaynak kodlu bir benzetim aracıdır [42]. NS-3, NS-2'nin bir güncellemesi değil onun yerini alacak bir benzetim aracı olarak değerlendirilmektedir [46]. NS-3, bazı NS-2 API (Application Programming Interface)'lerini desteklemez ve NS-2'den daha iyi olup halen geliştirilen bazı yeni özellikler içerir [42]. NS-2'den farklı olarak OTcl'i desteklemez [44]. Ağ benzetimleri C++ programlama diline ek olarak Python ile de gerçekleştirilebilir [15], [43]. Python nedeniyle sınırlı görselleştirme desteğine sahip olması, geriye dönük uyumlu olmadığından NS-2'den geçişlerin zor olması [42], IP ve MAC adresleri gibi ağ ayarlarının kolay yapılandırılması konusunda hala yetersiz kalması ve karmaşık yapısı nedeniyle zor öğrenilmesi [43] NS-3'ün kısıtlarındandır.

OMNeT++, C++ tabanlı açık kaynak kodlu bir benzetim aracıdır [47]. Ayrıca Java veya C# gibi alternatif dilleri de destekler [48]. Kapsamlı bir grafiksel kullanıcı ara yüzüne sahip OMNeT++ [44] ile kablolu ve kablosuz ağlar, kuyruk ağları ve bulut bilişim gibi ağlar modellenebilir [48]. Büyük ölçekli ağları sorunsuz bir şekilde desteklemesi, modellemeler için zengin bir sınıf kütüphanesi sunması, benzetim senaryolarının paralel çalıştırılmasına izin vermesi ve sonuçların analizi için grafiksel araçlar içermesi bu aracın özelliklerindendir [42]. Performans ölçümlerinin analizinin zayıf olması ve protokol çeşitliliğinin az olması da OMNeT++ aracının kısıtları arasında sayılabilir [42].

OPNET, ağların benzetimini gerçekleştirmek, performansını ölçmek ve değerlendirmek için kapsamlı bir geliştirme ortamı sunan literatürde kabul görmüş bir benzetim aracıdır [40]. OPNET ile, yerel alan ağı (LAN - Local Area Network), geniş alan ağı (WAN - Wide Area Network), internet ağı, mobil ağ, algılayıcı ağı ve uydu ağı gibi çok çeşitli ağ modelleri tasarlanabilir [49]. OPNET'i diğer ağ benzetim araçlarından ayıran temel fark gücü ve çok yönlülüğüdür [48]. OPNET, kullanımı oldukça kolaylaştıran üst düzey bir grafiksel arayüz içermesi [45], [48] ve hızlı benzetim yeteneklerine sahip olması [15], [45] nedeniyle bu çalışmada tercih edilmiştir.

Çizelge 3.1'de bu dört benzetim aracının genel kriterlere göre karşılaştırılması yapılmıştır.

Çizelge 3.1. Benzetim araçlarının karşılaştırılması [15], [43], [48].

Kriter	**NS-2**	**NS-3**	**OMNeT++**	**OPNET**
Lisans Türü	Açık Kaynak	Açık Kaynak	Açık Kaynak	Ticari
Programlama Dili	C++ ve OTcl	C++ ve Python	C++	C ve C++
Grafiksel Arayüz Desteği	Sınırlı	Orta Seviye	Üst Düzey	Üst Düzey
Desteklenen İşletim Sistemleri	GNU/Linux, FreeBSD, Mac OS X, Windows	GNU/Linux, FreeBSD, Mac OS X, Windows	Linux, Mac OS X, Windows	Linux, Windows
Kullanım Kolaylığı	Zor	Zor	Kolay	Kolay
Dokümantasyon	Mükemmel	Mükemmel	Mükemmel	Mükemmel
Ölçeklenebilirlik	Sınırlı (5 000 düğüm)	Geniş ölçekli	Sınırlı (3 000 düğüm)	Geniş ölçekli

3.2. KULLANILAN BENZETİM ARACI - OPNET

İlk kez 1986'da tasarlanan ve 2000 yılında genel kullanıma sunulan OPNET yüksek seviyeli bir ağ benzetim aracıdır [42]. Modelleme, benzetim ve analiz olarak üç temel işlev sunan [48] OPNET ile birçok farklı ağ modeli tasarlanabilir. Tasarlanan bir ağ modeli için farklı topolojilere, yönlendirmelere, trafiğe, yük parametrelerine dayalı olarak farklı senaryolar oluşturulabilir [50]. Bu senaryolar benzetim olarak çalıştırılarak birçok farklı istatistik verisi toplanabilir [49].

OPNET, bireysel benzetim çalışmalarını proje olarak adlandırır [50]. Her proje kendi içinde bir veya daha fazla senaryodan oluşur. Bir proje, belirli bir topolojinin bir dizi farklı yapılandırma ayarı altında benzetim çalışmalarının bir kümesi olarak tanımlanabilir [50]. Bir senaryo ise, bir topolojinin belirli bir yapılandırma ayarı altındaki tek bir benzetim çalışmasıdır [50].

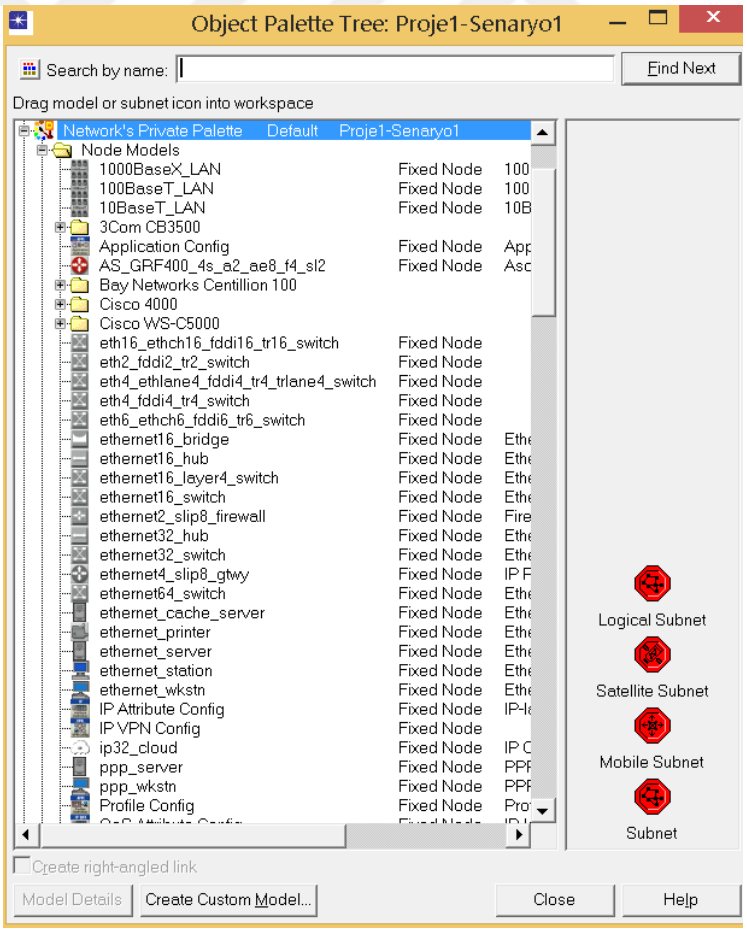
OPNET ile yeni projeler ve senaryoların oluşturulması, mevcut senaryoların çoğaltılması, bir senaryodan diğerine geçilmesi, bir veya birden fazla senaryo için benzetimlerin yapılandırılması ve çalıştırılması, farklı proje ve senaryolardan elde edilen benzetim sonuçlarının karşılaştırılması gibi birçok işlem kolaylıkla gerçekleştirilebilir [50].

Kendine özgü fonksiyonlardan oluşan bir C++ kütüphanesi içermesi ve C++ programlama dilini desteklemesi sayesinde OPNET, oluşturulan modelin kullanıcı

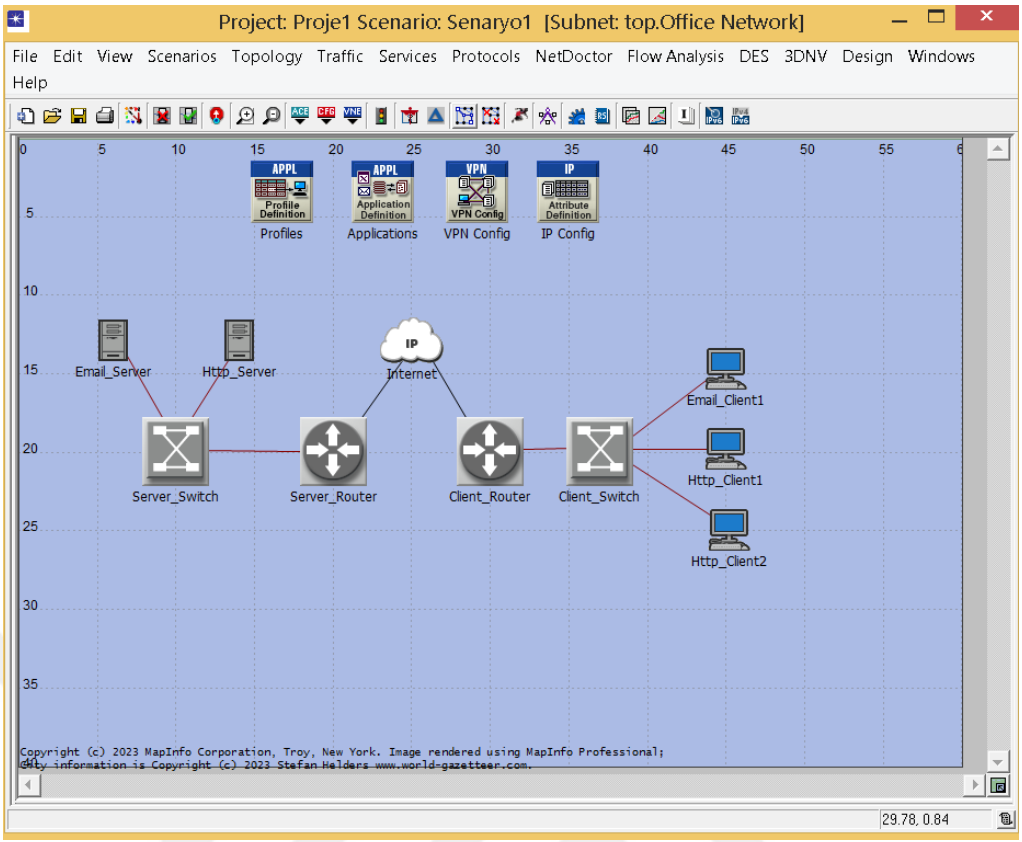
tarafından çok detaylı bir şekilde kontrol edilmesine olanak verir [51]. OPNET, modelleme ve benzetim görevlerini gerçekleştirmek için kullanıcılara bir dizi hiyerarşik kullanıcı arayüzü sunar [52].

3.2.1. Proje Editörü

Ağ benzetim projeleri ve senaryolarının yönetildiği ana kullanıcı arayüzüdür [49]. Ağ topolojisinin kapsamlı model kütüphanesi bileşenleriyle grafiksel olarak tasarlanmasını sağlar. Bunun için Şekil 3.1'deki nesne paletinden ağ düğümleri, alt ağlar, bağlantılar, profil yapılandırma ve uygulama yapılandırma gibi nesnelerin proje editörüne sürükle bırak ile yerleştirilmesi gerekir. Bir düğüm sabit, hareketli veya uydu düğümü olabilir. Kullanılan model parametrelerinin yapılandırılması; toplanacak istatistik verilerinin belirlenmesi; senaryoların tanımlanması, düzenlenmesi ve çalıştırılması; benzetim sonuçlarının görüntülenmesi ve karşılaştırılması gibi işlemler proje editörü ile gerçekleştirilir [49]. Şekil 3.2'de OPNET proje editörü gösterilmiştir.



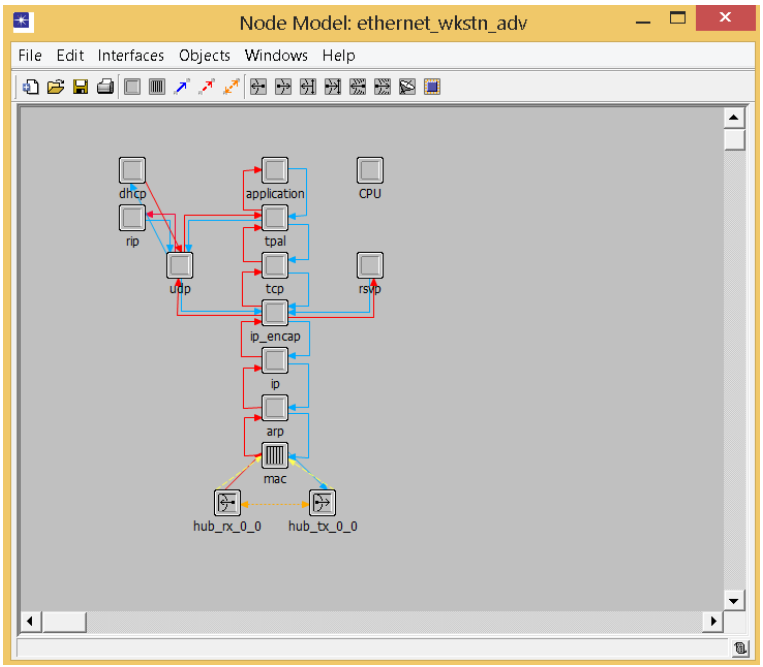
Şekil 3.1. Nesne paleti.



Şekil 3.2. Proje editörü.

3.2.2. Düğüm Editörü

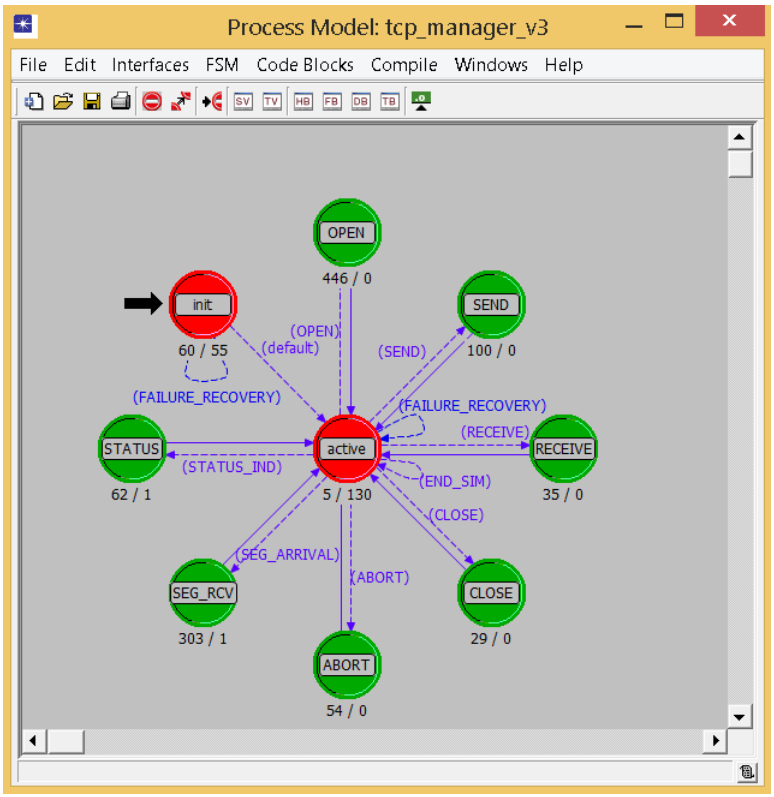
Bir düğümün iç yapısının düzenlenmesini sağlayan kullanıcı arayüzüdür [49]. Bir düğüm bir istemciyi, bir sunucuyu, bir anahtar cihazını, bir yönlendiriciyi veya bir alt ağı temsil edebilir. Her düğüm, her biri o düğümün belirli bir işlevini temsil eden birkaç modülden oluşur. Bu modüller birbirleriyle paket akışları veya istatistik akışları aracılığıyla iletişim kurabilirler [53]. Şekil 3.3'te Ethernet Workstation nesnesi için düğüm editörü gösterilmiştir.



Şekil 3.3. Düğüm editörü.

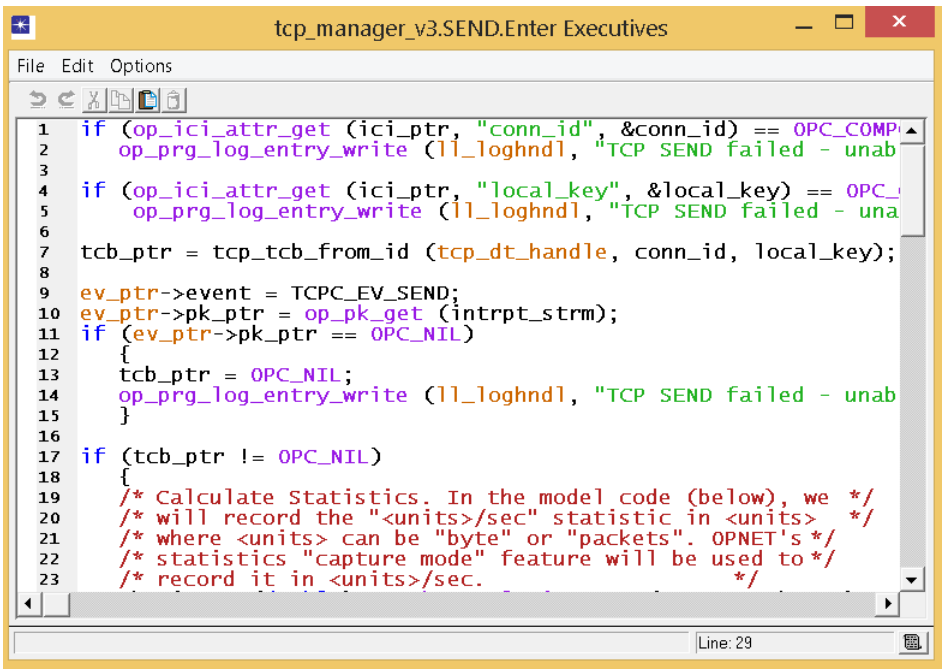
3.2.3. İşlem editörü:

Algoritmaları ve protokolleri uygulamak için kod yazılan yer işlem editörüdür [49]. OPNET işlem editörü, işlemleri güçlü bir durum-geçiş diyagramı yaklaşımı kullanarak gösterir. Durumlar ve geçişler, olaylara yanıt olarak bir işlemin ilerlemesini grafiksel olarak tanımlar [53]. Her durum, iletişim protokollerini programlamaya yönelik genişletilmiş bir fonksiyon kütüphanesi tarafından desteklenen C kodu içerir [52]. Şekil 3.4'te OPNET işlem editöründe örnek bir işlemin durum-geçiş diyagramı gösterilmiştir.

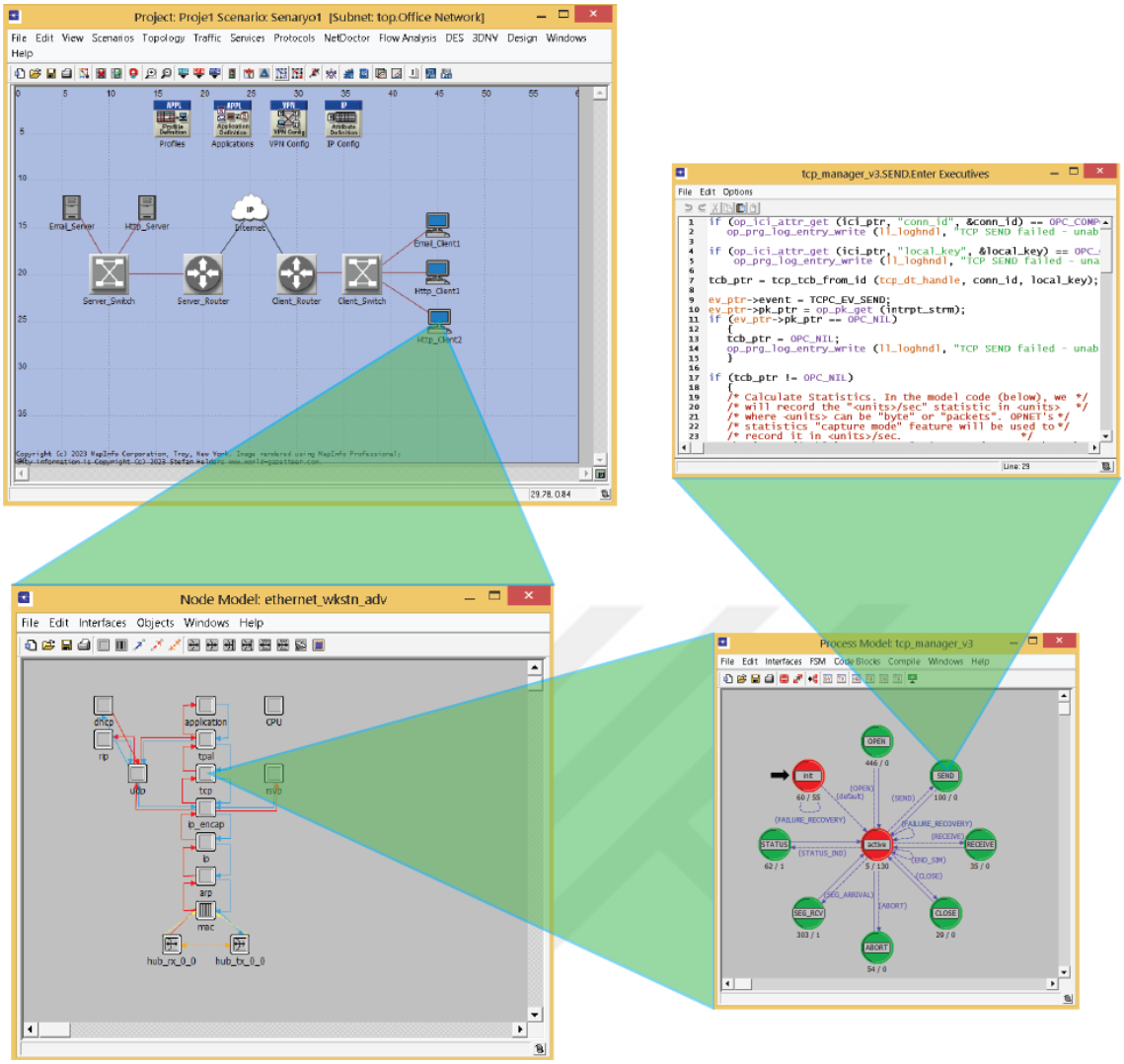


Şekil 3.4. İşlem editörü.

Şekil 3.4'teki örnek işlemin SEND durumuna ait kaynak C kodu ise Şekil 3.5'te verilmiştir. Şekil 3.6'da ise OPNET'te proje editörü, düğüm editörü, işlem editörü ve kaynak C kodu arasındaki hiyerarşik yapı gösterilmiştir.

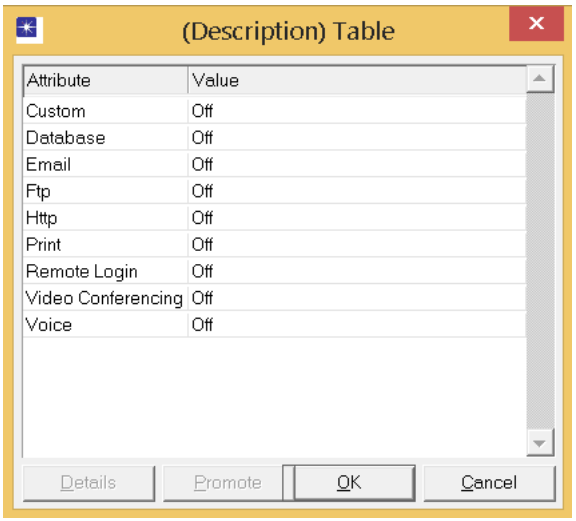


Şekil 3.5. SEND durumu kaynak C kodu.



Şekil 3.6. OPNET editör hiyerarşisi.

OPNET benzetim aracında HTTP, FTP, e-mail, veritabanı, Print, Remote Login, video konferans ve VoIP uygulamaları varsayılan uygulamalar olarak tanımlanmıştır. OPNET uygulama tanımlama tablosu Şekil 3.7'de gösterilmiştir. Bu çalışmada OPNET benzetim aracının 14.5 sürümü ile video konferans uygulaması kullanılmıştır.



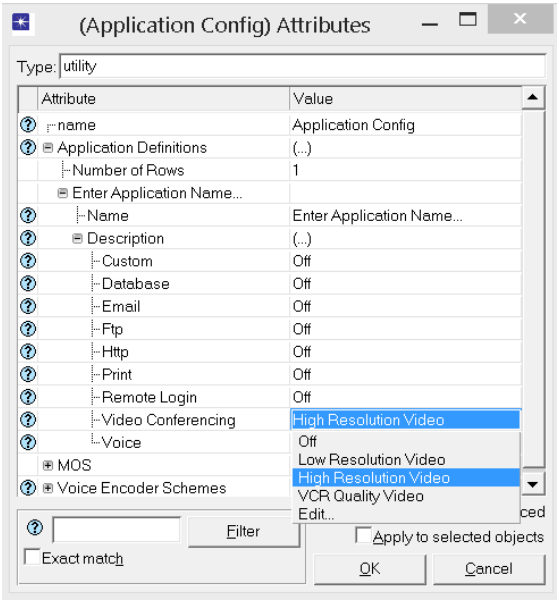
Şekil 3.7. OPNET uygulama tanımlama tablosu.

3.3. BENZETİM İÇİN GEREKLİ OLAN VİDEO PARAMETRELERİ

OPNET benzetim aracı, video konferans uygulaması için Çizelge 3.2'de gösterilen üç varsayılan değeri sunmaktadır. Bu değerlerin OPNET üzerindeki ayarlaması Şekil 3.8'de gösterildiği gibi gerçekleştirilmektedir.

Çizelge 3.2. OPNET varsayılan video konferans değerleri.

Değer	**Çözünürlük (Piksel x Piksel)**	**Paket boyutu (bayt)**	**FPS (Saniyedeki video karesi)**
Düşük Çözünürlüklü Video	128 x 120	17 280	10
Yüksek Çözünürlüklü Video	128 x 240	34 560	15
VCR Kalitesi Video	352 x 240	253 440	30

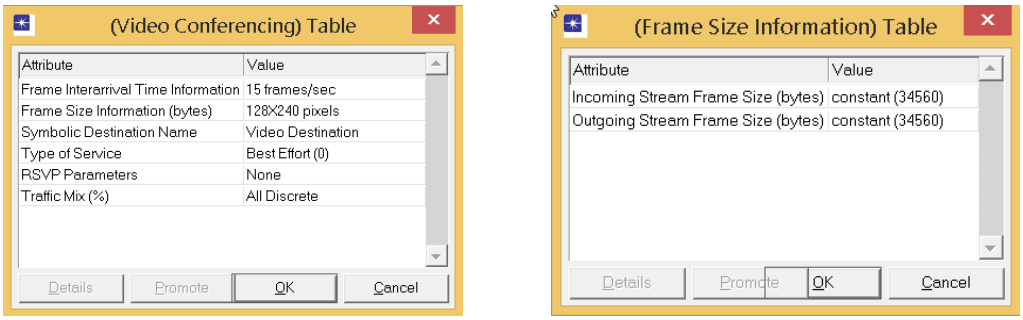


Şekil 3.8. OPNET video konferans değerleri.

Bu çalışmada video konferans uygulamasının benzetimi Yüksek Çözünürlüklü ve Özel Çözünürlüklü olmak üzere iki farklı video çözünürlük değeriyle gerçekleştirilmiştir.

3.3.1. Yüksek Çözünürlüklü Video

Yüksek Çözünürlüklü Video OPNET benzetim aracının video konferans uygulamasında sunmuş olduğu varsayılan bir değerdir. Bu değer kullanıldığında bir video karesinin paket boyutu 34 560 bayt olmakta ve ağ üzerinden saniyede 15 video karesinin iletimi yapılmaktadır. Yüksek Çözünürlüklü Video konferans parametrelerinin OPNET üzerindeki gösterimi Şekil 3.9'da gösterilmiştir.



a) b)

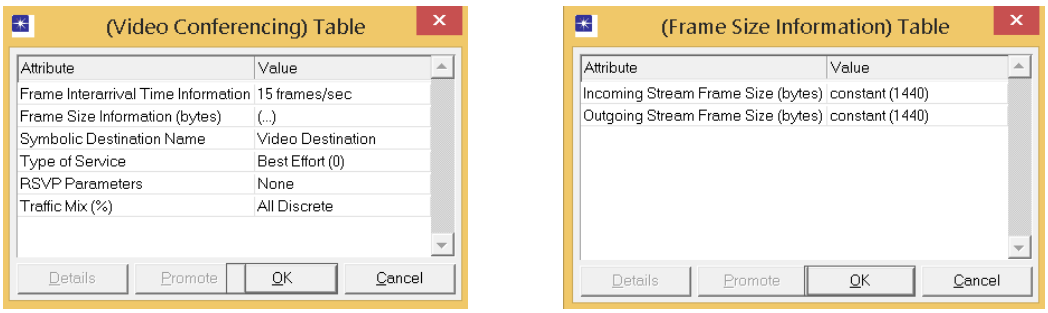
Şekil 3.9. Yüksek Çözünürlüklü Video konferans parametreleri

a) Genel değerler b) Paket boyutu

3.3.2. Özel Çözünürlüklü Video

Yüksek Çözünürlüklü Video değerinin kullanılması, OPNET ile video konferans uygulamasında VPN kullanımı engellemektedir. Çünkü OPNET aracı, VPN bağlantısını L2TP (Layer 2 Tunneling Protocol) VPN modelini kullanarak gerçekleştirmekte ve bundan dolayı ağdaki veri paketleri boyutunun en yüksek Ethernet iletim birimi değeri olan 1 500 bayttan az olması gerekmektedir. Aksi halde paket kayıpları meydana gelmektedir. Bu durum OPNET ile video konferans uygulamasında VPN kullanımını gerçekleştirebilmek için yeni bir çözünürlük belirleme gerekliliğini ortaya çıkarmıştır.

OPNET benzetim aracı, video konferans uygulamasında video karesi paket boyutunun değiştirilerek çözünürlüğün özelleştirilmesine imkân vermektedir [49]. Bu tez çalışmasında, video karesi paket boyutunun 1 440 bayt olarak belirlendiği yeni bir video çözünürlüğü oluşturulmuş ve Özel Çözünürlüklü Video olarak isimlendirilmiştir. Bu yeni çözünürlük değerinde ağ üzerinde bir saniyede iletilen video karesi sayısı değiştirilmeyerek 15 olarak kullanılmıştır. Özel Çözünürlüklü Video değerinin kullanılması ile OPNET'te video konferans uygulamasında VPN kullanımı sağlanmıştır. Özel Çözünürlüklü Video konferans parametrelerinin OPNET üzerindeki yapılandırması Şekil 3.10'da gösterilmiştir.



a) b)

Şekil 3.10. Özel Çözünürlüklü Video konferans parametreleri

a) Genel değerler b) Paket boyutu

4. DENEYSEL ÇALIŞMA

Bu bölümde öncelikle bu tez çalışmasında modellenen senaryolar ve ilgili topolojiler hakkında bilgi verilmiş daha sonra benzetim süresince toplanacak istatistik verileri gösterilmiştir. Devamında, benzetimin gerçekleştiriminden bahsedilmiş ve benzetim sonuçlarının grafiksel olarak gösterimi yapılmıştır. Son olarak grafiksel gösterimler video konferans uygulama performansı açısından analiz edilmiştir.

4.1. BENZETİMİN MODELLEMESİ

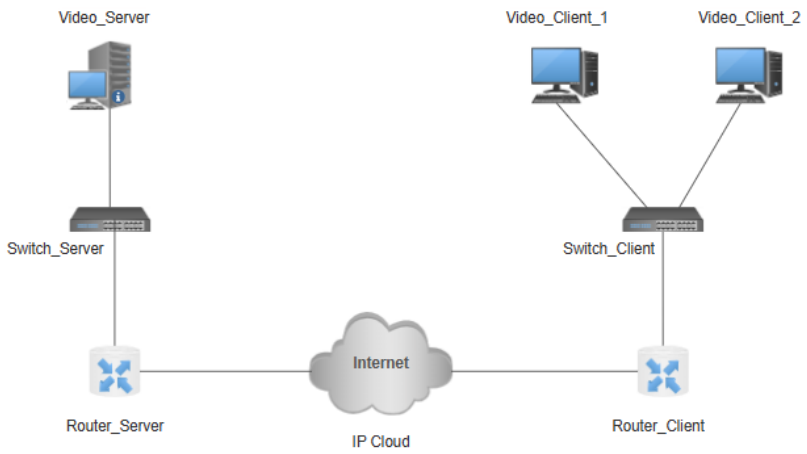
Bu çalışmada video konferans uygulamalarının benzetimi Yüksek Çözünürlüklü Video (Bölüm 3.3.1) ve Özel Çözünürlüklü Video (Bölüm 3.3.2) olarak iki farklı çözünürlük değeriyle gerçekleştirilmiştir. Modellemede LAN ve WLAN ağ teknolojileri kullanılmıştır. LAN teknolojisinde IEEE 802.3 standardı ile 100 Mbps veri hızı, WLAN teknolojisinde ise IEEE 802.11g standardı ile 54 Mbps veri hızı kullanılmıştır. Çalışmada modellenen senaryolar Çizelge 4.1'de gösterilmiştir.

Çizelge 4.1. Video konferans senaryoları.

Senaryo Adı	Ağ Teknolojisi	Video Çözünürlüğü	Güvenlik Çözümü
Senaryo 1	LAN	Yüksek Çözünürlük	-
Senaryo 2			Güvenlik Duvarı
Senaryo 3	WLAN		-
Senaryo 4			Güvenlik Duvarı
Senaryo 5	LAN	Özel Çözünürlük	-
Senaryo 6			Güvenlik Duvarı
Senaryo 7			VPN
Senaryo 8	WLAN		-
Senaryo 9			Güvenlik Duvarı
Senaryo 10			VPN

Senaryo 1

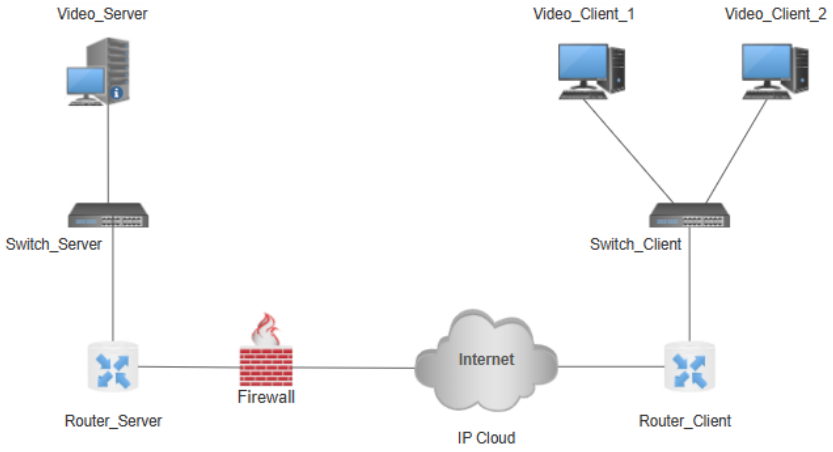
Bu senaryo için oluşturulan topoloji Şekil 4.1'de verildiği gibi modellenmiştir. Bu topolojide, üç katılımcının yer aldığı Yüksek Çözünürlüklü Video değerinin kullanıldığı bir video konferans görüşmesi gerçekleşmektedir. Topolojide, iki adet video konferans istemcisi (Video_Client_1 ve Video_Client_2) bir yerel alan ağında bulunmakta ve anahtar cihazına (Switch_Client) bağlanmaktadır. Bu anahtar cihazı da yönlendiriciye (Router_Client) bağlanmaktadır. Bir adet video konferans sunucusu (Video_Server) kurumsal bir ağda bulunmakta, anahtar cihazına (Switch_Server) ve bir yönlendiriciye (Router_Server) bağlanmaktadır. Yönlendiricilerin 1 Gbps hızındaki fiber kablolarla internet bulutuna (IP Cloud) bağlanmakta olduğu bu senaryoda herhangi bir güvenlik duvarı veya VPN bağlantısı kullanılmamaktadır.



Şekil 4.1. Senaryo 1'in topolojisi.

Senaryo 2

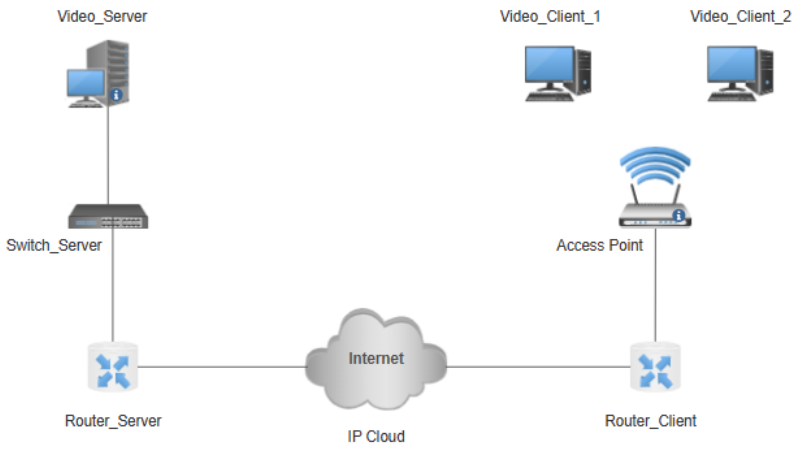
Bu senaryonun Senaryo 1'den farkı topolojiye eklenen güvenlik duvarıdır. Bu senaryoda topolojideki Router_Server adlı yönlendirici nesnesi ile ve IP Cloud adlı internet bulutu nesneleri arasına Firewall adlı bir güvenlik duvarı nesnesi eklenmiştir. Güvenlik duvarı nesnesi üzerinde gerekli yapılandırma ayarları yapılmıştır. Senaryoya ait topoloji Şekil 4.2'de gösterilmiştir.



Şekil 4.2. Senaryo 2'nin topolojisi.

Senaryo 3

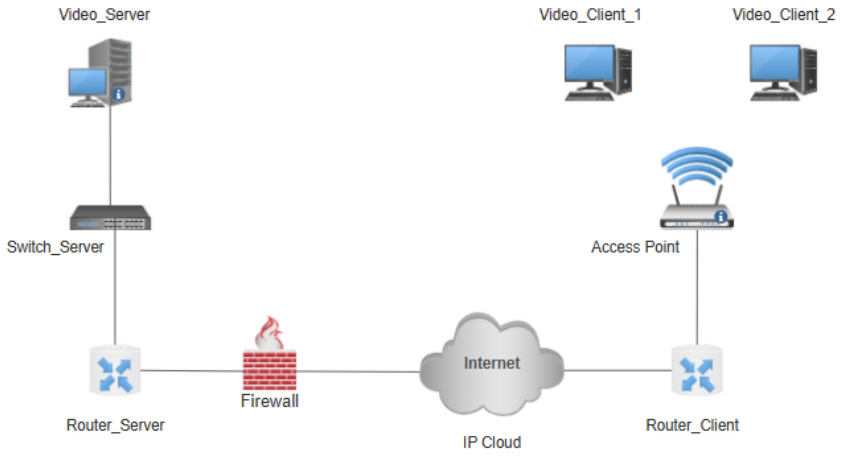
Bu senaryoya ait topoloji Şekil 4.3'teki gibi modellenmiştir. Yüksek Çözünürlüklü Video değerinin kullanıldığı ve üç video konferans katılımcısının yer aldığı bu topolojide iki adet video konferans istemcisi (Video_Client_1 ve Video_Client_2) bir WLAN'da bulunmaktadır. Bu istemciler 54 Mbps hızındaki kablosuz bağlantıyla AP (Access Point)'e bağlanmakta, AP ise 100 Mbps hızındaki ağ kablosuyla yönlendiriciye (Router_Client) bağlanmaktadır. Topolojide bir adet video konferans sunucusu (Video_Server) kurumsal bir ağda bulunmakta ve 100 Mbps hızındaki ağ kablosuyla anahtar cihazına (Switch_Server) bağlanmaktadır. Bu anahtar 100 Mbps hızındaki ağ kablosu ile bir yönlendiriciye (Router_Server) bağlanmaktadır. Her iki yönlendirici 1 Gbps hızındaki fiber kablolarla internet bulutuna (IP Cloud) bağlanmaktadır.



Şekil 4.3. Senaryo 3'ün topolojisi.

Senaryo 4

Bu senaryonun modellemesi, Senaryo 3'e ait Şekil 4.3'teki topolojideki Router_Server adlı yönlendirici ve IP Cloud adlı internet bulutu nesneleri arasına Firewall adında bir güvenlik duvarı nesnesi eklenerek oluşturulmuştur. Güvenlik duvarı nesnesi üzerinde gerekli yapılandırma ayarları yapılarak video konferans trafiğinin geçişine izin verilmiştir. Bu senaryoya ait topoloji Şekil 4.4'te gösterilmiştir.



Şekil 4.4. Senaryo 4'ün topolojisi.

Senaryo 5

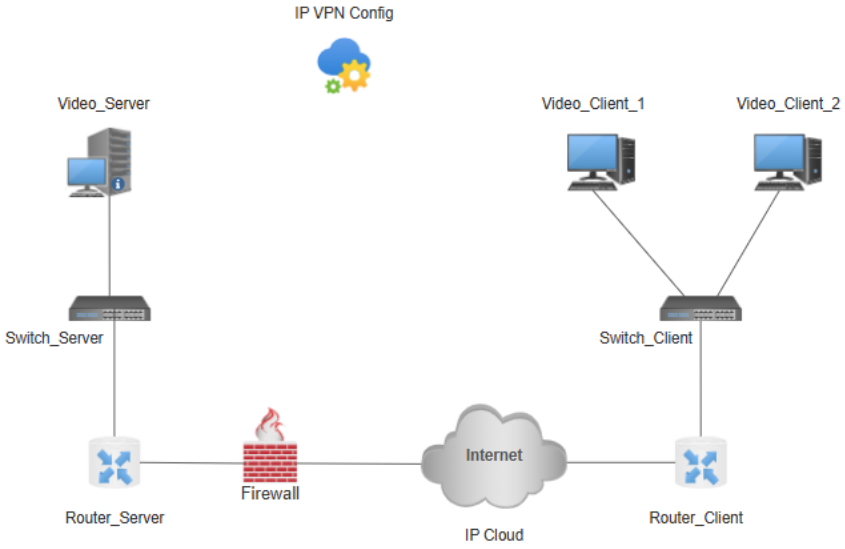
Bu senaryoya ait topoloji Senaryo 1'e ait Şekil 4.1'teki topolojinin aynısıdır. Bu senaryodaki tek farklılık Yüksek Çözünürlüklü Video değerinin yerine Özel Çözünürlüklü Video değerinin kullanılmış olmasıdır.

Senaryo 6

Bu senaryoya ait topoloji Senaryo 2'ye ait Şekil 4.2'deki topolojinin aynısıdır. Bu senaryoda Senaryo 2'den farklı olarak Yüksek Çözünürlüklü Video değeri yerine Özel Çözünürlüklü Video değeri kullanılmıştır.

Senaryo 7

Bu senaryo Şekil 4.2'teki topolojiye IP VPN yapılandırma nesnesinin eklenmesiyle oluşturulmuştur. Video konferans trafiğinin VPN bağlantısı üzerinden sağlanması için güvenlik duvarı ve IP VPN nesnelerinde gerekli yapılandırma ayarları yapılmıştır. Topolojisi Şekil 4.5'te verilen bu senaryoda video konferans değeri olarak Özel Çözünürlüklü Video değeri kullanılmıştır.



Şekil 4.5. Senaryo 7'nin topolojisi.

Senaryo 8

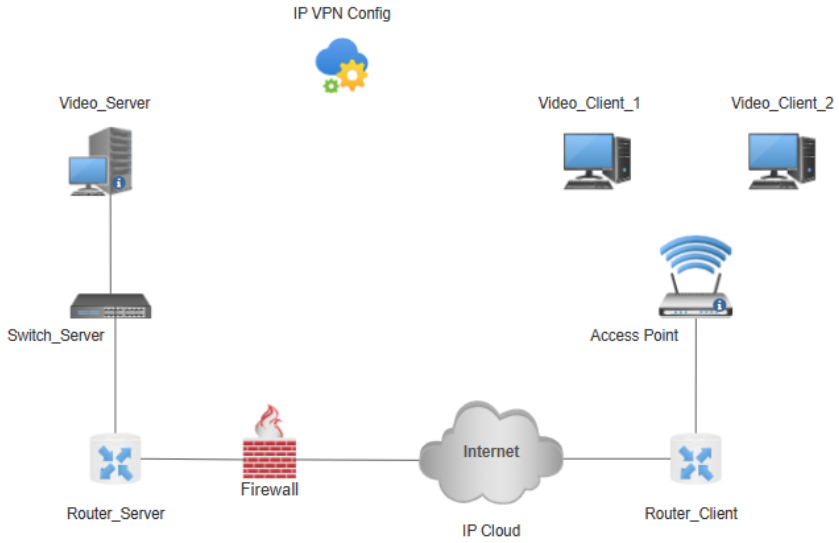
Bu senaryonun Senaryo 3'ten farkı Yüksek Çözünürlüklü Video değerinin yerine Özel Çözünürlüklü Video değerinin kullanılmış olmasıdır. Bu senaryonun topolojisi Senaryo 3'e ait Şekil 4.3'teki topolojinin aynısıdır.

Senaryo 9

Bu senaryo ait topoloji Senaryo 4'e ait Şekil 4.4'teki topolojinin aynısıdır. Bu senaryoda Senaryo 4'den farklı olarak video konferans uygulaması Yüksek Çözünürlüklü Video değeri yerine Özel Çözünürlüklü Video değeri kullanılarak gerçekleştirilmiştir.

Senaryo 10

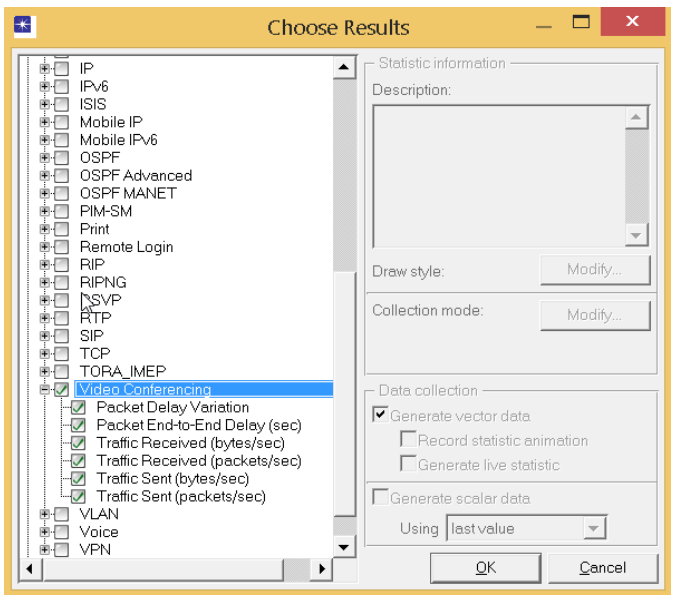
Özel Çözünürlüklü Video değerinin kullanıldığı bu senaryo, Şekil 4.4'teki topolojiye IP VPN yapılandırma nesnesi eklenerek oluşturulmuştur. Topolojisi Şekil 4.6'da gösterilen bu senaryoda video konferans trafiğinin güvenlik duvarı üzerinden değil VPN bağlantısı üzerinden sağlanması için gerekli yapılandırma ayarları yapılmıştır.



Şekil 4.6. Senaryo 10'un topolojisi.

4.2. BENZETİMDE TOPLANAN İSTATİSTİK VERİLERİ

Senaryolara ait topolojilerin modellemesi yapıldıktan sonra benzetim sırasında toplanacak istatistik verileri seçilmiştir. Bunun için proje editöründeki DES menüsündeki Choose Individual Statistics seçeneğine tıklanarak Şekil 4.7'de gösterilen veri seçim ekranına erişilmiştir.



Şekil 4.7. Veri seçim ekranı.

OPNET benzetim aracında üç tür istatistik verisi bulunmaktadır [49].

1. Genel: Bir istatistik verisinin ağın tamamından toplanan değerini gösterir [50].
2. Düğüm: Bir istatistik verisinin ağdaki tek bir düğümden toplanan değerini gösterir.
3. Bağlantı: Ağdaki tek bir bağlantıdan toplanan istatistik verilerini gösterir.

Bu çalışmada senaryoların benzetimi süresince toplanan istatistik verileri Çizelge 4.2'de verilmiştir.

Çizelge 4.2. Toplanan istatistik verileri.

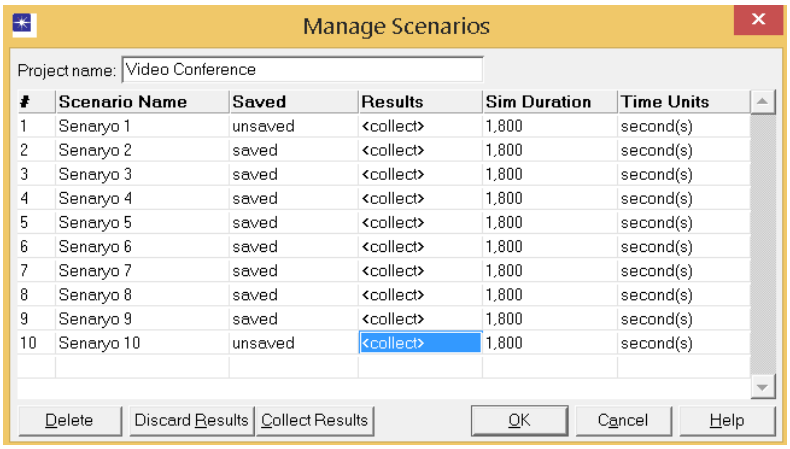
İstatistik Türü	**İstatistik Grubu**	**İstatistik Adı**	**Açıklama**	**Ölçü Birimi**
Genel	Video Konferans	Packet End-to-End Delay	Uçtan Uca Gecikme Süresi	sn.
Genel	Video Konferans	Packet Delay Variation	Gecikme Varyasyonu	sn.
Genel	Video Konferans	Traffic Received	Saniyede Alınan Paket Sayısı	paket/sn.
Genel	Video Konferans	Traffic Received	Saniyede Alınan Veri Miktarı	bayt/sn.
Genel	Video Konferans	Traffic Sent	Saniyede Gönderilen Paket Sayısı	paket/sn.
Genel	Video Konferans	Traffic Sent	Saniyede Gönderilen Veri Miktarı	bayt/sn.
Düğüm	Görüntülü Arayan Taraf	Packet End-to-End Delay	Uçtan Uca Gecikme Süresi	sn.
Düğüm	Görüntülü Arayan Taraf	Packet Delay Variation	Gecikme Varyasyonu	sn.
Düğüm	Görüntülü Arayan Taraf	Traffic Received	Saniyede Alınan Paket Sayısı	paket/sn.
Düğüm	Görüntülü Arayan Taraf	Traffic Received	Saniyede Alınan Veri Miktarı	bayt/sn.
Düğüm	Görüntülü Arayan Taraf	Traffic Sent	Saniyede Gönderilen Paket Sayısı	paket/sn.

Çizelge 4.2 (devamı). Toplanan istatistik verileri.

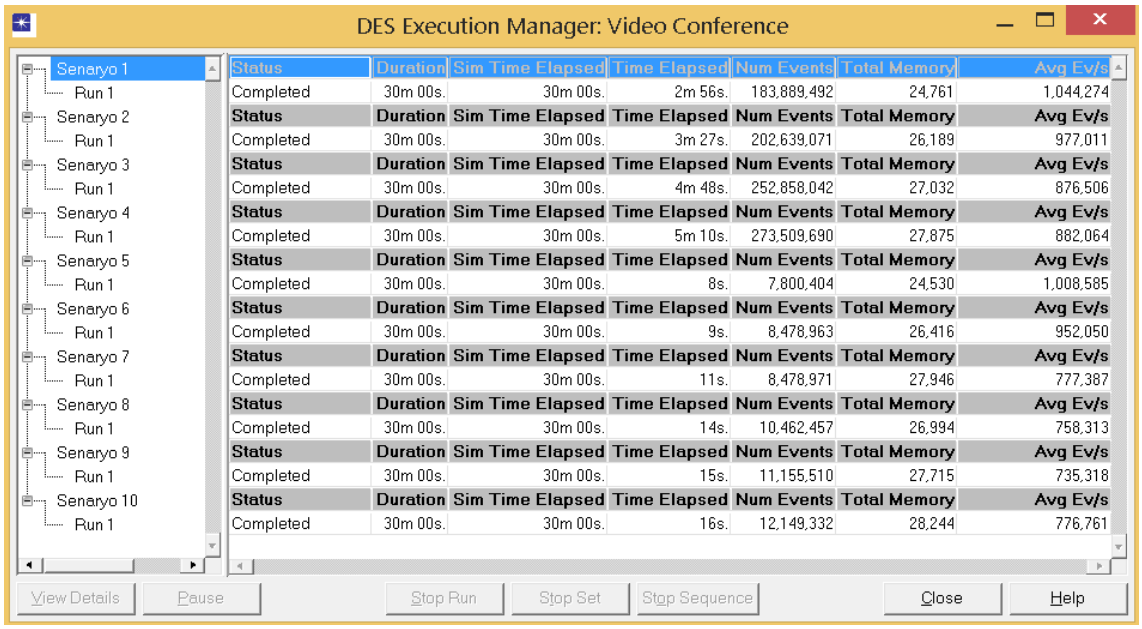
Düğüm	Görüntülü Arayan Taraf	Traffic Sent	Saniyede Gönderilen Veri Miktarı	bayt/sn.
Düğüm	Görüntülü Aranan Taraf	Packet End-to-End Delay	Uçtan Uca Gecikme Süresi	sn.
Düğüm	Görüntülü Aranan Taraf	Packet Delay Variation	Gecikme Varyasyonu	sn.
Düğüm	Görüntülü Aranan Taraf	Traffic Received	Saniyede Alınan Paket Sayısı	paket/sn.
Düğüm	Görüntülü Aranan Taraf	Traffic Received	Saniyede Alınan Veri Miktarı	bayt/sn.
Düğüm	Görüntülü Aranan Taraf	Traffic Sent	Saniyede Gönderilen Paket Sayısı	paket/sn.
Düğüm	Görüntülü Aranan Taraf	Traffic Sent	Saniyede Gönderilen Veri Miktarı	bayt/sn.

4.3. VİDEO KONFERANSLARIN PERFORMANS ANALİZİ

Modellemenin tamamlanmasından sonra, Çizelge 4.2'de gösterilen benzetim esnasında toplanacak istatistik verileri belirlenmiştir. Senaryoların benzetim süresini belirlemek için daha önceki bazı çalışmalardan faydalanılmıştır. Benzetim senaryoları [54]'te 900 sn., [55]'de 1 800 sn., [37] ve [56]'da 3 600 sn. çalıştırılmıştır. Yapılan bu çalışmada ise her senaryo 1 800 sn. çalıştırılarak benzetimi gerçekleştirilmiştir. Bunun için proje editöründeki Scenarios menüsünden Manage Scenarios seçeneğine tıklanarak ulaşılan senaryo yönetim ekranı Şekil 4.8'de gösterilmiştir. Bu ekranda OK butonuna basılmasıyla senaryolarının benzetimlerinin anlık çalışma durumlarını gösteren Şekil 4.9'da gösterilen ekran açılmıştır. Benzetim sonunda toplanan istatistik verileri grafiğe dönüştürülerek; video konferans uygulamalarında güvenlik duvarı ve VPN kullanımının farklı ağlardaki etkileri uygulama performansı açısından değerlendirilmiştir.



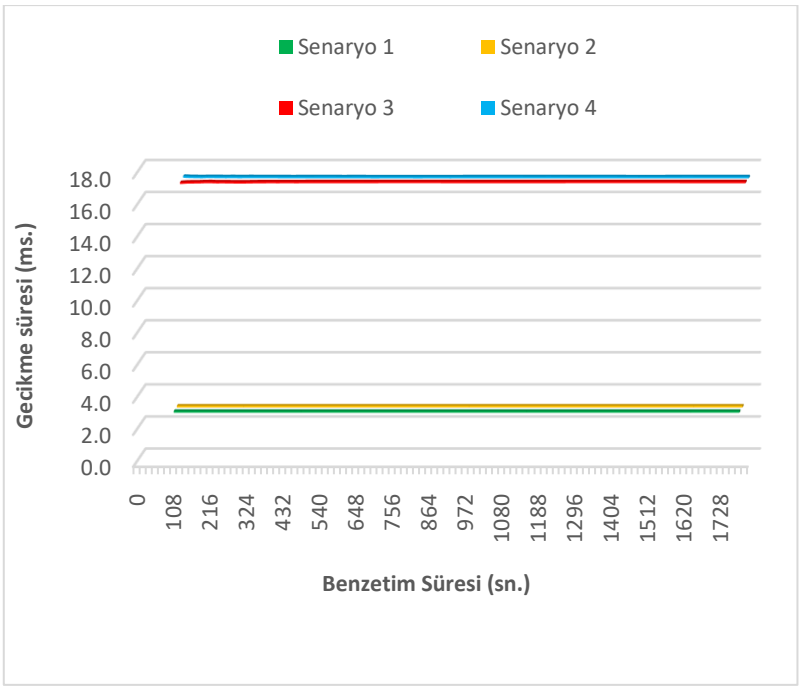
Şekil 4.8. Senaryo yönetim ekranı.



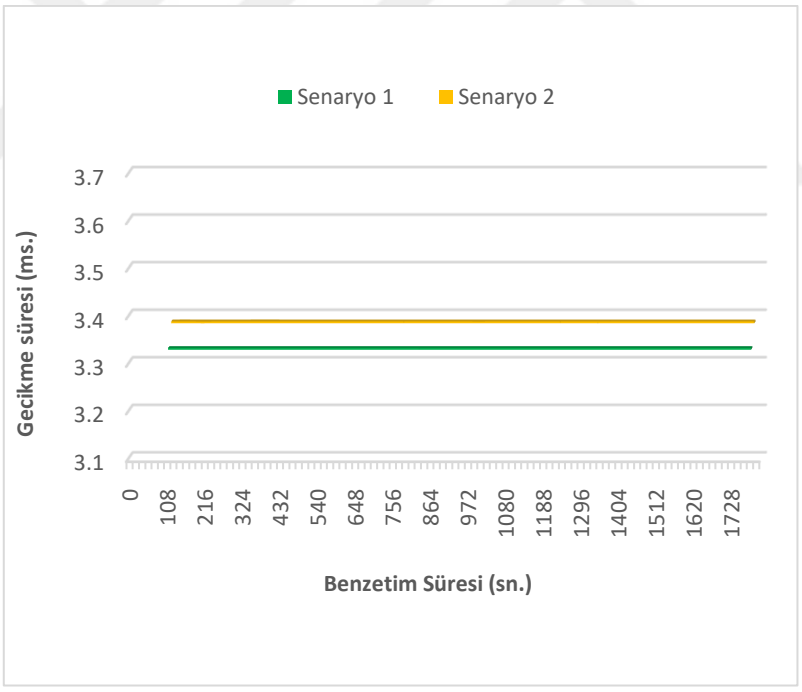
Şekil 4.9. Benzetim çalıştırma yönetim ekranı.

4.3.1. Uçtan Uca Gecikme Süresi

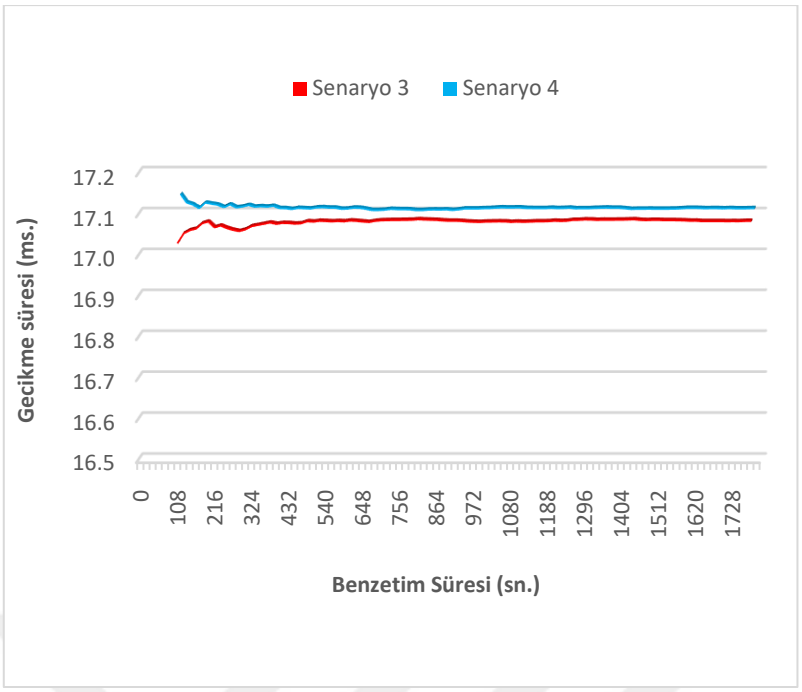
Şekil 4.10'da, Yüksek Çözünürlüklü Video değeri ile benzetimi gerçekleştirilen Senaryo 1, Senaryo 2, Senaryo 3 ve Senaryo 4 için ortalama uçtan uca gecikme süresi gösterilmiştir. Buna göre WLAN kullanıldığında paket gecikme süresi yaklaşık 14 ms. artmıştır. Senaryo.1 ve Senaryo 2, Şekil 4.11'de gösterildiği gibi kendi aralarında karşılaştırıldığında güvenlik duvarı kullanımının uçtan uca gecikme süresini artırdığı gözlenmiştir. Şekil 4.12'de gösterildiği gibi Senaryo 3 ve Senaryo 4 de kendi aralarında karşılaştırılmış ve yine güvenlik duvarı kullanımının uçtan uca gecikme süresinde artışa sebep olduğu gözlemlenmiştir.



Şekil 4.10. Senaryo 1, 2, 3 ve 4'ün uçtan uca gecikme süresi.

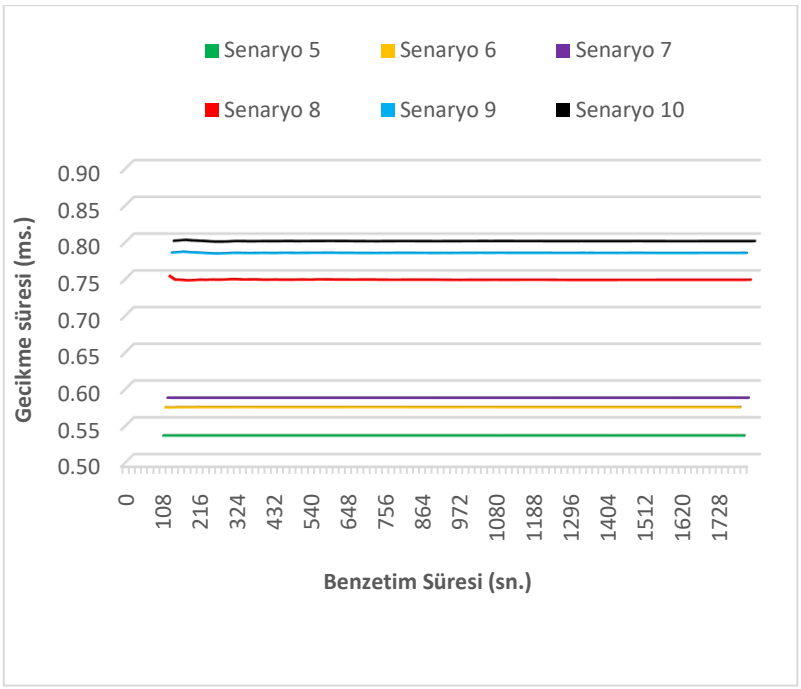


Şekil 4.11. Senaryo 1 ve 2'nin uçtan uca gecikme süresi.

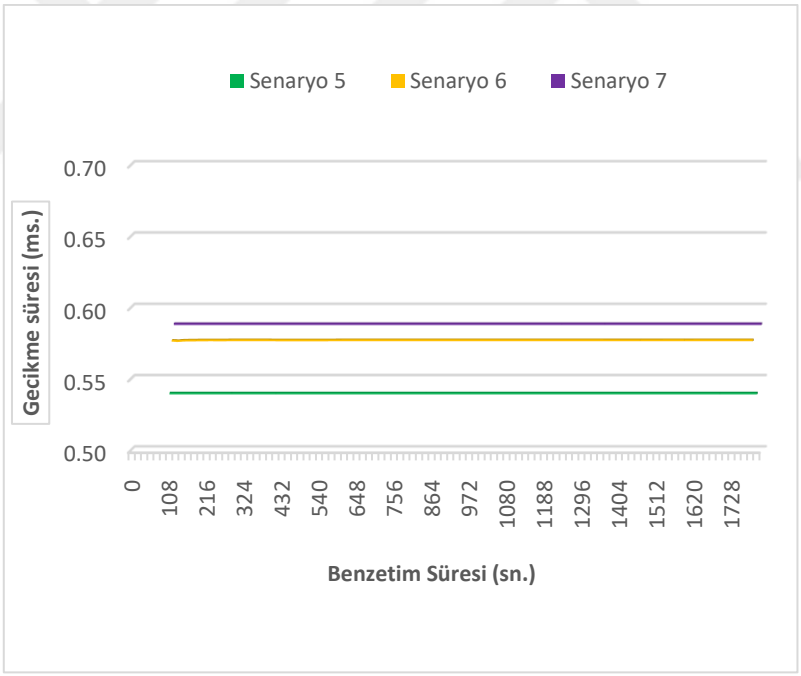


Şekil 4.12. Senaryo 3 ve 4'ün uçtan uca gecikme süresi.

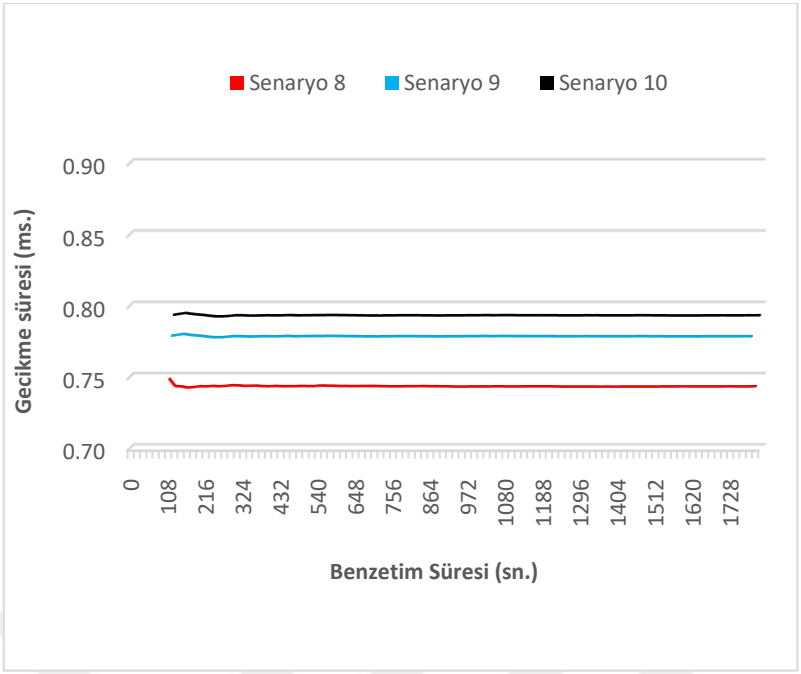
Özel Çözünürlüklü Video değeri kullanılarak benzetimi gerçekleştirilen tüm senaryolar için ortalama uçtan uca paket gecikme süresi Şekil 4.13'te gösterilmiştir. Buna göre video konferans istemcilerinin LAN yerine WLAN'da bulunması paket gecikme süresini 0,2 ms. civarında artırmaktadır. Ayrıca güvenlik duvarı ve VPN kullanımının hem LAN hem de WLAN kullanılan senaryolarda uçtan uca gecikmeyi arttırdığı görülmektedir. LAN kullanılan Senaryo 5, Senaryo 6 ve Senaryo 7 Şekil 4.14'teki gibi; WLAN kullanılan Senaryo 8, Senaryo 9 ve Senaryo 10 da Şekil 4.15'te gösterildiği gibi kendi aralarında karşılaştırılmıştır. Her iki karşılaştırmada da VPN kullanımının güvenlik duvarı kullanımına göre uçtan uca gecikmeyi daha fazla artırdığı gözlemlenmiştir.



Şekil 4.13. Senaryo 5, 6, 7, 8, 9, 10'nun uçtan uca gecikme süresi.



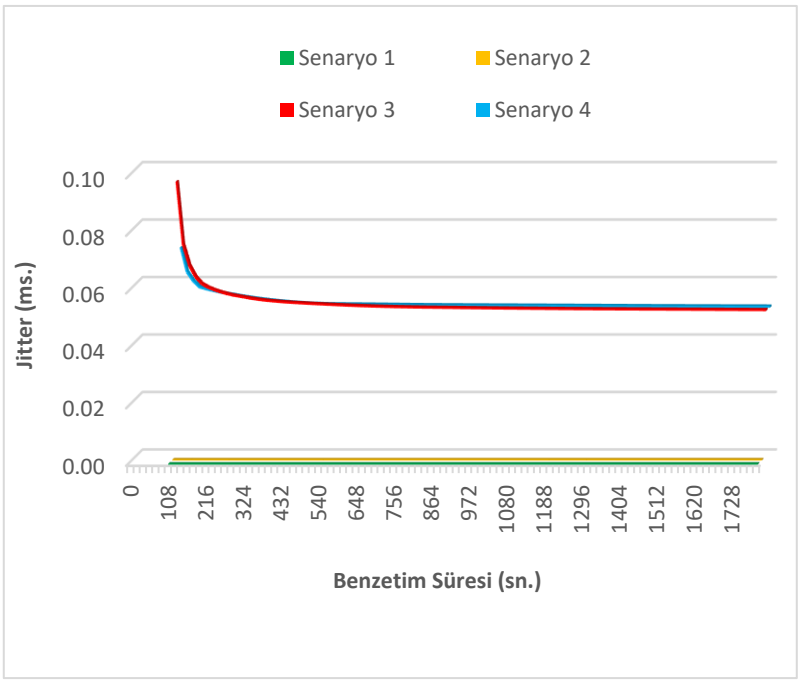
Şekil 4.14. Senaryo 5, 6 ve 7'nin uçtan uca gecikme süresi.



Şekil 4.15. Senaryo 8, 9 ve 10'un uçtan uca gecikme süresi.

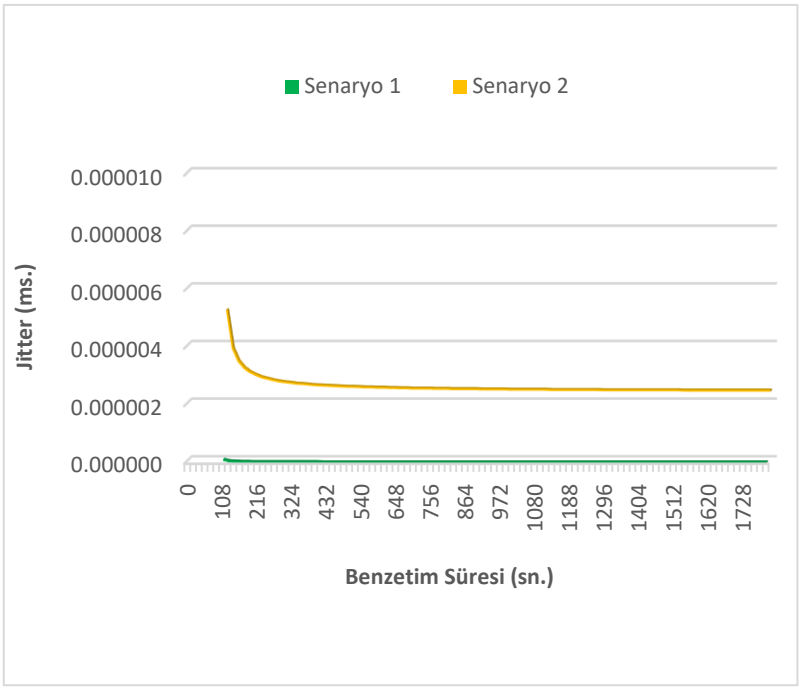
4.3.2. Paket Gecikme Varyasyonu (Jitter)

Yüksek Çözünürlüklü Video değeri kullanılarak benzetimi gerçekleştirilen senaryoların ortalama paket gecikme varyasyonu, Şekil 4.16'da tek bir grafikte gösterilmiştir. Buna göre WLAN kullanılan senaryolardaki paket gecikme varyasyonu değerinin, LAN kullanılan senaryolardakinden yaklaşık 0,05 ms. daha fazla olduğu görülmektedir.



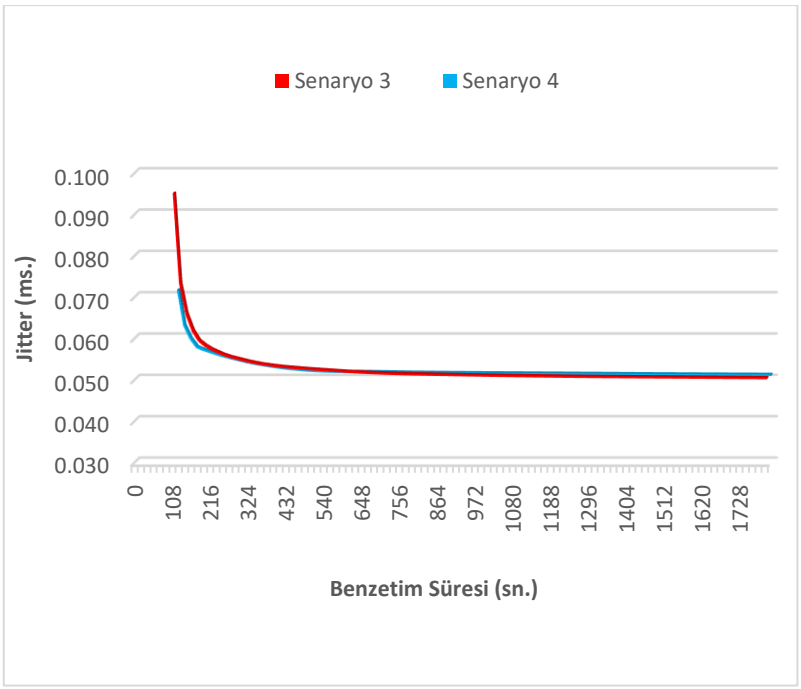
Şekil 4.16. Senaryo 1, 2, 3 ve 4'ün paket gecikme varyasyonu.

Şekil 4.17'de, Senaryo 1 ve Senaryo 2'nin kendi aralarında paket gecikme varyasyonu karşılaştırılması gösterilmiştir. Buna göre, güvenlik duvarı kullanılmadığında paket gecikme varyasyonu sıfır olmaktayken güvenlik duvarı kullanıldığında paket gecikme varyasyonu yaklaşık 0,0000023 ms. değerini almaktadır.



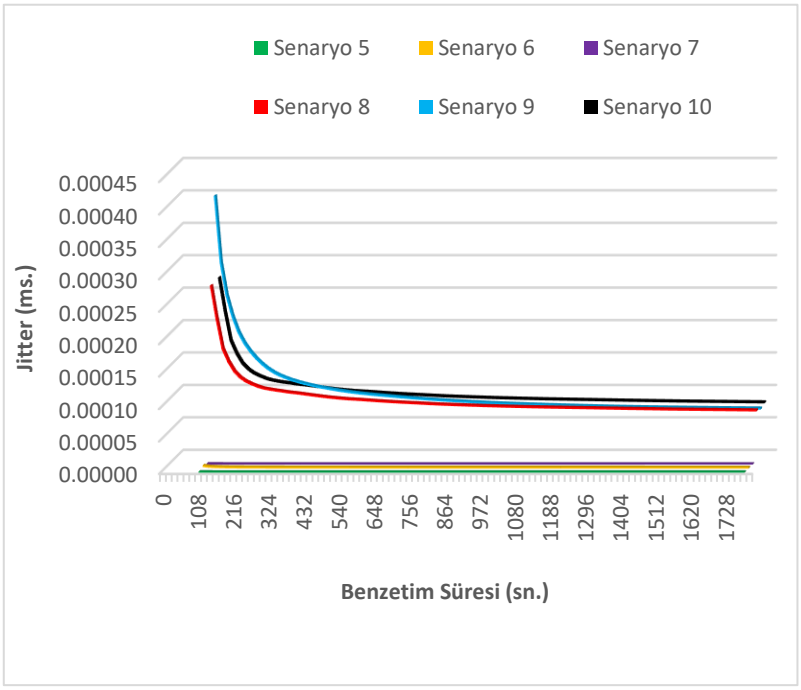
Şekil 4.17. Senaryo 1 ve 2'nin paket gecikme varyasyonu.

Senaryo 3 ve Senaryo 4 kendi aralarında paket gecikme varyasyonu açısından karşılaştırıldığında Şekil 4.18'de gösterildiği gibi kayda değer bir fark gözlemlenmemiştir.



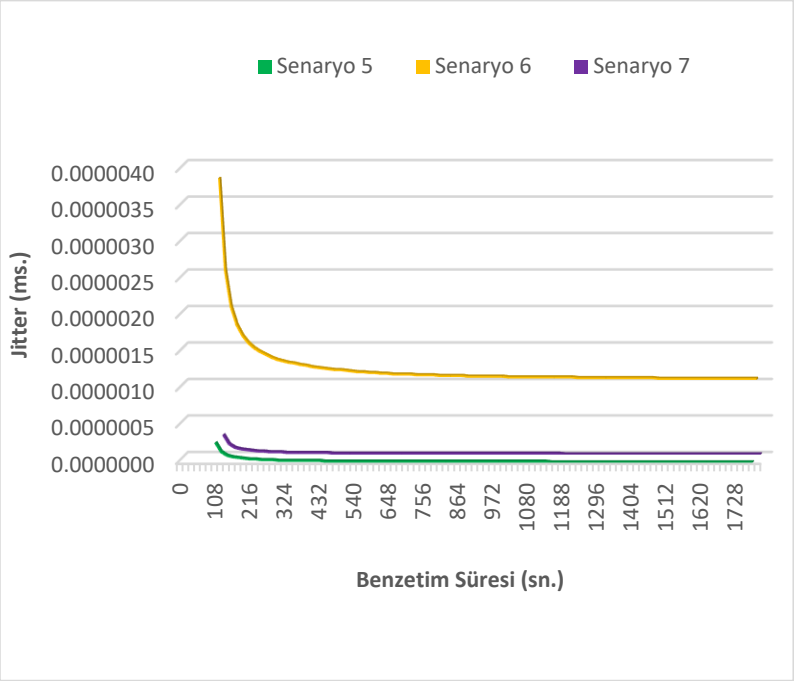
Şekil 4.18. Senaryo 3 ve 4'ün paket gecikme varyasyonu.

Özel Çözünürlüklü Video değeri ile benzetimi gerçekleştirilen senaryoların ortalama paket gecikme varyasyonu, Şekil 4.19'da gösterilmiştir. Buna göre paket gecikme varyasyonu, WLAN kullanılan senaryolarda 0,00008 ms. değerine çok yakın iken LAN kullanılan senaryolarda sıfıra çok yakındır.



Şekil 4.19. Senaryo 5, 6, 7, 8, 9 ve 10'un paket gecikme varyasyonu.

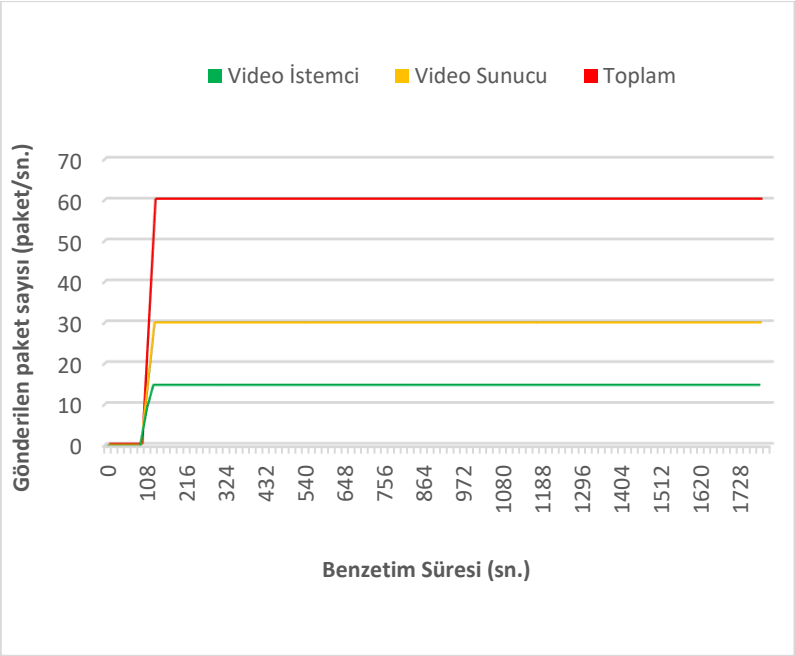
Özel Çözünürlüklü Video değerinin kullanıldığı senaryolardan video konferans istemcilerinin LAN'da bulunduğu senaryoların kendi aralarında paket gecikme varyasyonu karşılaştırılması Şekil 4.20'de gösterilmiştir. Buna göre; güvenlik duvarı kullanımı paket gecikme varyasyonunu 0,000001 ms. artırırken VPN kullanımı paket gecikme varyasyonu etkilememiştir. WLAN kullanılan senaryolar ise paket gecikme varyasyonu açısından kendi aralarında belirgin bir farklılık göstermemiştir.



Şekil 4.20. Senaryo 5, 6 ve 7'nin paket gecikme varyasyonu.

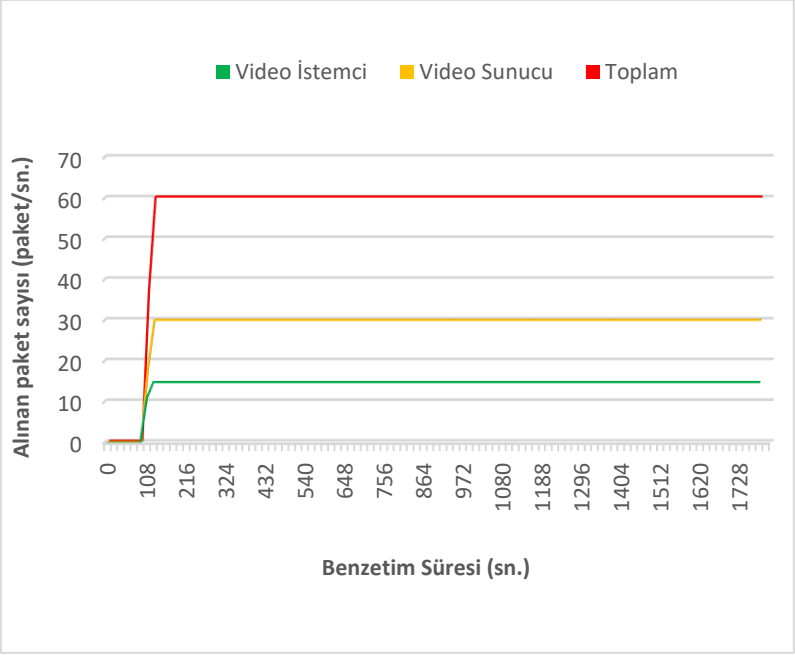
4.3.3. Gönderilen ve Alınan Paket Sayıları

Gönderilen paket sayısı, video konferans görüşmesinde bir saniyede gönderilen paket sayısını ifade eder. Benzetimi gerçekleştirilen tüm senaryolar için bir video istemcisi, video sunucusu ve tüm katılımcılar tarafından gönderilen paket sayısı değerleri Şekil 4.21'de gösterilmiştir. Video konferans istemcilerinin her biri saniyede 15 video paketi iletmekteyken, video sunucusu ise, her bir istemciye saniyede 15 video paketi olmak üzere toplam 30 video paketi iletmektedir. Video konferans görüşmesi katılımcıları tarafından bir saniyede gönderilen toplam paket sayısı ise 60 değerini almıştır.



Şekil 4.21. Tüm senaryolara ait gönderilen paket sayısı.

Tüm senaryolarda bir video istemcisi, video sunucusu ve katılımcıların tümü tarafından alınan paket sayısı değerleri ise Şekil 4.22'de gösterilmiştir. Buna göre her bir video istemcisi saniyede 15, video sunucusu ise saniyede 30 video paketi almaktadır. Konferans görüşmesi katılımcıları tarafından bir saniyede alınan toplam paket sayısı ise beklenildiği gibi 60 olarak ölçülmüştür.

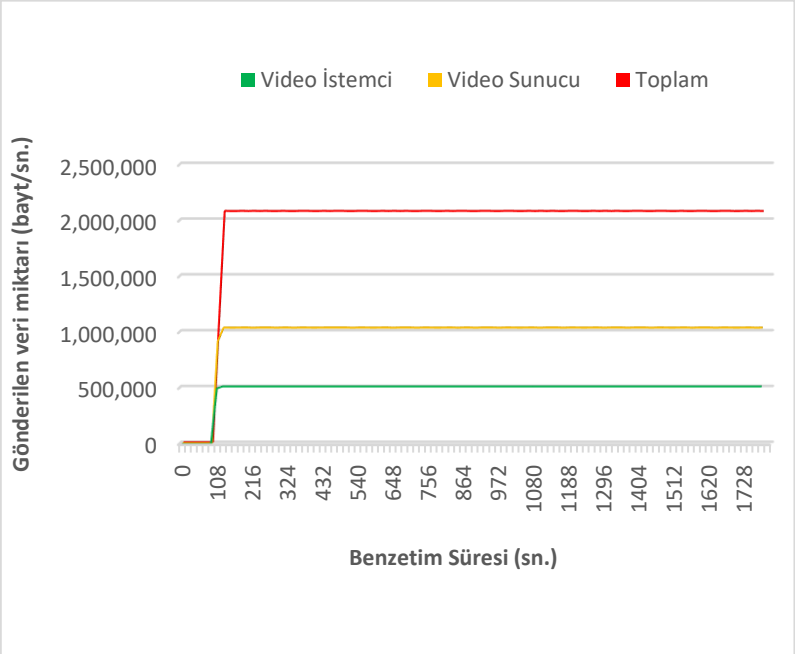


Şekil 4.22. Tüm senaryolara ait alınan paket sayısı.

Senaryoların benzetimleri sonucunda gönderilen ve alınan paket sayıları olarak beklenilen değerler ölçülmüş olup herhangi bir paket kaybı meydana gelmemiştir.

4.3.4. Gönderilen ve Alınan Veri Miktarı

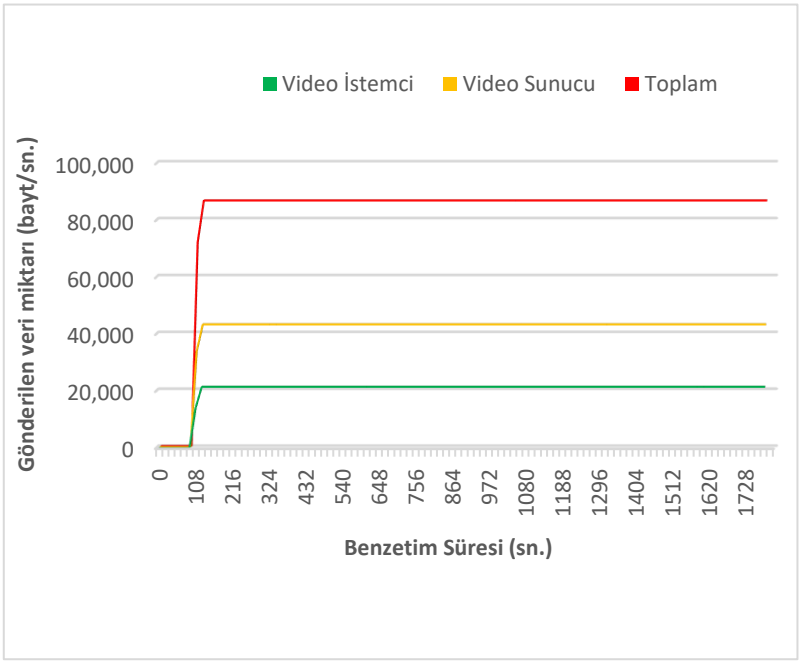
Şekil 4.23, Yüksek Çözünürlüklü Video değerinin kullanıldığı senaryolar için bir istemciye, sunucuya ve ağdaki tüm katılımcılara ait bir saniyede gönderilen veri miktarını göstermektedir. Bu grafiğe göre her bir video istemcisi saniyede 518 400 bayt, video sunucusu ise saniyede 1 036 800 bayt video verisi göndermektedir. Tüm video konferans katılımcıları tarafından ise saniyede toplam 2 073 600 baytlık veri gönderilmektedir. Yüksek Çözünürlüklü Video değeri kullanıldığında her biri 34 560 bayt büyüklüğündeki video paketlerinden her bir istemci saniyede 15 paket, sunucu saniyede 30 paket, katılımcıların tümü ise saniyede toplam 60 paket veri gönderdiğinden benzetim, beklenilen sonuçları üretmiştir.



Şekil 4.23. Yüksek Çözünürlüklü Video senaryolarında gönderilen veri miktarı.

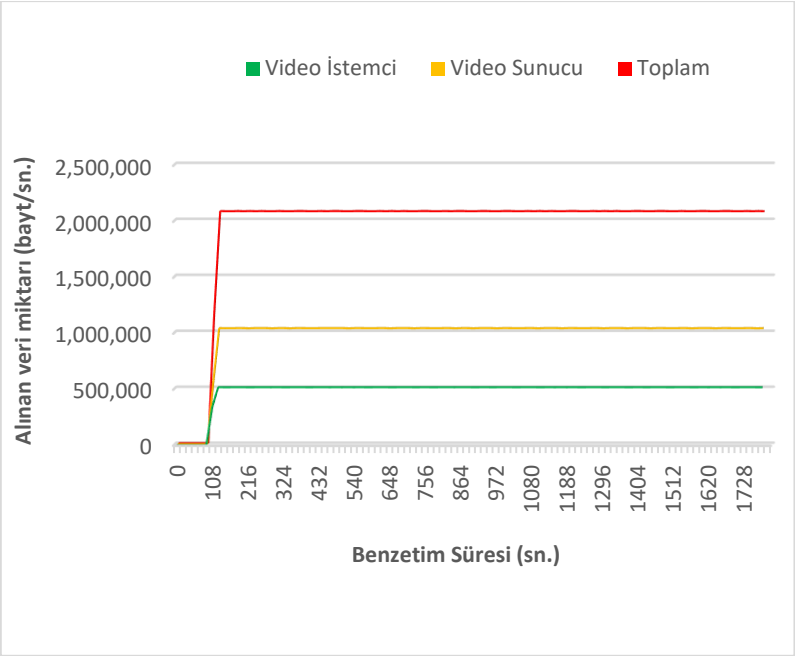
Özel Çözünürlüklü Video değerinin kullanıldığı senaryolar için bir istemciye, sunucuya ve ağdaki tüm katılımcılara ait bir saniyede gönderilen veri miktarı ise Şekil 4.24'te gösterilmektedir. Buna göre bir istemciden saniyede 21 600 baytlık veri iletilmekteyken sunucudan saniyede toplam 43 200 baytlık video verisi iletilmektedir. Konferans görüşmesi katılımcılarının tamamı tarafından ise saniyede 86 400 bayt veri iletilmektedir. Özel Çözünürlüklü Video değeri kullanılan senaryolarda her biri 1 440 bayt boyutunda

olan video paketlerinden saniyede her bir istemci 15 paket, sunucu 30 paket, tüm katılımcılar ise toplam 60 paket veri göndermektedir.



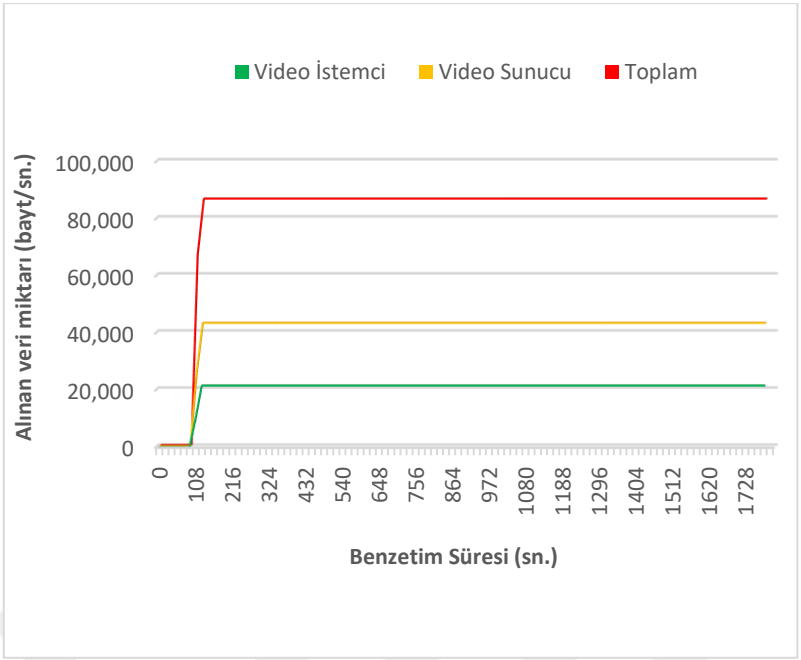
Şekil 4.24. Özel Çözünürlüklü Video senaryolarında gönderilen veri miktarı.

Yüksek Çözünürlüklü Video değerinin kullanıldığı senaryolar için bir istemciye, sunucuya ve ağdaki tüm katılımcılara ait bir saniyede alınan veri miktarı Şekil 4.25'te gösterilmektedir. Buna göre her bir video istemcisi saniyede 518 400 bayt, video sunucusu saniyede 1 036 800 bayt, tüm katılımcılar ise saniyede toplam 2 073 600 bayt veri almaktadır. Her bir video paketinin boyutunun 34 560 bayt olduğu Yüksek Çözünürlüklü Video senaryolarında saniyede her bir istemci 15 paket, sunucu 30 paket, tüm katılımcılar ise toplam 60 paket veri almaktadır.



Şekil 4.25. Yüksek Çözünürlüklü Video senaryolarında alınan veri miktarı.

Şekil 4.26, Özel Çözünürlüklü Video değerinin kullanıldığı senaryolarda bir istemciye, sunucuya ve tüm katılımcılara ait bir saniyede alınan veri miktarını göstermektedir. Buna göre bir istemci saniyede 21 600 baytlık, sunucu ise saniyede 43 200 baytlık video verisi almaktadır. Katılımcıların tümü ise saniyede 86 400 bayt veri almaktadır. Özel Çözünürlüklü Video değeri kullanılan senaryolarda her biri 1 440 bayt boyutunda olan video paketlerinden saniyede her bir istemci 15 paket, sunucu 30 paket, tüm katılımcılar ise toplam 60 paket veri almaktadır.



Şekil 4.26. Özel Çözünürlüklü Video senaryolarında alınan veri miktarı.

Bu çalışmada benzetimi gerçekleştirilen tüm senaryolar için gönderilen ve alınan veri miktarları birbiriyle uyumlu olup herhangi bir veri kaybı gerçekleşmemiştir.

4.4. PERFORMANS DEĞERLENDİRMESİ

Bu çalışmada ilk önce video konferans uygulamalarında güvenlik duvarı kullanımının uçtan uca gecikmeye etkisi incelenmiştir. Yüksek Çözünürlüklü Video değeri ve LAN teknolojisinin kullanıldığı Senaryo 1 ile Senaryo 2 karşılaştırıldığında güvenlik duvarı kullanımı 0,046 ms. gecikme artışına neden olmuştur. Yüksek Çözünürlüklü Video değeri ve WLAN teknolojisinin kullanıldığı Senaryo 3 ile Senaryo 4 karşılaştırıldığında güvenlik duvarı kaynaklı gecikme artışı 0,035 ms. olmuştur. Özel Çözünürlüklü Video değeri ve LAN kullanılan Senaryo 5 ile Senaryo 6 karşılaştırıldığında güvenlik duvarı kullanımının uçtan uca gecikmeyi 0,035 ms. artırdığı gözlemlenmiştir. Özel Çözünürlüklü Video değeri ve WLAN kullanılan Senaryo 8 ile Senaryo 9 karşılaştırıldığında güvenlik duvarı kullanımı 0,032 ms. gecikme artışına neden olmuştur.

Çalışmada daha sonra video konferans uygulamalarında güvenlik duvarı kullanımının paket gecikme varyasyonunu ne şekilde etkilediği araştırılmıştır. Senaryo 1 ve Senaryo 2 karşılaştırıldığında güvenlik duvarı kullanımı paket gecikme varyasyonunda 0,0000025 ms. artışa sebep olmuştur. WLAN teknolojisinin kullanıldığı Senaryo 3 ve Senaryo 4 karşılaştırıldığında güvenlik duvarı kaynaklı paket gecikme varyasyonu artışı

gözlemlenmemiştir. Güvenlik duvarı kaynaklı paket gecikme varyasyonu artışı Senaryo 5 ve Senaryo 6 karşılaştırıldığında 0,0000012 ms. iken Senaryo 8 ve Senaryo 9 karşılaştırıldığında 0,000006 ms. değerini almıştır.

Bu çalışmada video konferans uygulamasında VPN kullanımı sadece Özel Çözünürlüklü Video değeri ile gerçekleştirilmiş ve VPN kullanımının uçtan uca gecikmeye etkisi incelenmiştir. LAN teknolojisinin kullanıldığı Senaryo 5 ve Senaryo 7 karşılaştırıldığında VPN kullanımının uçtan uca gecikmeyi 0,045 ms. artırdığı gözlemlenmiştir. WLAN kullanılan Senaryo 8 ve Senaryo 10 karşılaştırıldığında ise VPN kullanımı uçtan uca gecikmeyi 0,046 ms. artırmıştır.

Video konferans uygulamalarını VPN bağlantısı ile kullanmanın paket gecikme varyasyonuna etkilerini belirlemek için Senaryo 5 ve Senaryo 7 karşılaştırıldığında paket gecikme varyasyonu değeri her iki senaryoda da sıfır olarak tespit edilmiştir. Senaryo 8 ve Senaryo 10 karşılaştırıldığında ise paket gecikme varyasyonu değeri her ikisi için 0,00009 ms. olarak ölçülmüştür.

Çalışmada kullanılan farklı ağ teknolojileri uçtan uca gecikme süresi yönünden incelendiğinde; WLAN kullanılan Senaryo 3, LAN kullanılan Senaryo 1'den 13,75 ms. daha fazla uçtan uca gecikme oluşturmuştur. WLAN kullanılan Senaryo 8 ise LAN kullanılan Senaryo 5'ten 0,21 ms. daha fazla uçtan uca gecikme oluşturmuştur.

LAN ve WLAN ağ teknolojilerinin paket gecikme varyasyonuna etkisi incelendiğinde, Senaryo 3'te Senaryo 1'den 0,053 ms. daha fazla gecikme varyasyon değerleri elde edilmiştir. Senaryo 8 ise Senaryo 5'ten 0,00009 ms. daha fazla paket gecikme varyasyonu üretmiştir.

Bu çalışmada, kullanılan farklı video çözünürlük değerlerinin uçtan uca gecikmeye etkisi de değerlendirilmiştir. Uçtan uca gecikme süresi Yüksek Çözünürlüklü Video değeri kullanılan Senaryo 1'de 3,33 ms. iken Özel Çözünürlüklü Video değeri kullanılan Senaryo 5'te 0,54 ms. olarak ölçülmüştür.

Çalışmada paket gecikme varyasyonu Yüksek Çözünürlüklü Video değeri kullanılan Senaryo 2'de 0,0000025 ms., Özel Çözünürlüklü Video değeri kullanılan Senaryo 6'da ise 0,0000012 ms. olarak ölçülmüştür.

Benzetimi gerçekleştirilen tüm senaryolarda gönderilen ve alınan paket sayıları ile veri miktarları incelendiğinde video paketlerinin iletiminin başarıyla sağlandığı ve herhangi bir paket kaybı meydana gelmediği gözlemlenmiştir.

Bu çalışmada benzetimi gerçekleştirilen tüm senaryolar uçtan uca gecikme, gecikme varyasyonu ve paket kayıp değerleri açısından kabul edilebilir değerleri sağlamaktadır. Yani modellenen tüm senaryolarda video konferans görüşmeleri kaliteli bir biçimde gerçekleşmiştir.

5. SONUÇ

Ağ üzerinden kullanılan uygulamaların performansında hem kullanılan ağ teknolojilerinin hem de güvenlik duvarı ve VPN gibi güvenlik çözümlerinin bazı etkileri olduğu bilinmektedir. Bu çalışmada, video konferans uygulamalarının LAN ve WLAN ağlarında güvenlik duvarı ve VPN ile kullanımı benzetim yöntemiyle gerçekleştirmiştir. Modellenen senaryolarda iki farklı video çözünürlük değeri kullanıldığından çözünürlüğün performansa etkileri de analiz edilebilmiştir. Benzetim sonuçlarının görsel olarak karşılaştırılmasıyla, ilgili ağ teknolojilerinde güvenlik duvarı ve VPN kullanımının video konferans uygulama performansına olan etkileri değerlendirilmiştir.

5.1. SONUÇ

Bu çalışmada, güvenlik duvarı kullanımının video konferans uygulamalarında uçtan uca gecikme ve gecikme varyasyonu değerlerinde artışa sebep olduğu bulunmuştur. Bununla birlikle elde edilen değerler uygulama performansı açısından kabul edilebilir üst sınırların oldukça altındadır. Yani bu çalışmada güvenlik duvarı kullanılan tüm senaryolarda kaliteli video konferans görüşmeleri gerçekleştirilebilmiştir. Güvenlik duvarı, kendi üzerinden geçen tüm paketleri daha önceden tanımlanmış kurallara göre filtrelemektedir. Kurallara uyan paketlerin geçişine izin verilirken kurallara uymayan paketler engellenmektedir. Gerçekleştirilen bu filtreleme işleminin paketlerin iletiminde fazladan gecikmeye dolayısıyla uçtan uca gecikmede artışa sebep olduğu açıktır. Paket gecikme varyasyonu ardışık iki paketin kaynaktan hedefe ulaşma süreleri arasındaki farkı ifade eder. Aynı anda hedefe ulaşması gereken ardışık iki paket için güvenlik duvarında gerçekleşen filtreleme işlem süresinin aynı olması son derece düşük bir ihtimaldir.

Video konferans uygulamalarında VPN kullanımı ile uçtan uca gecikmenin arttığı, paket gecikme varyasyonunun ise etkilenmediği bulgusu bu çalışmanın diğer bir sonucudur. Benzetim sonucunda elde edilen değerler kabul edilebilir üst sınırların oldukça altında olup VPN kullanımı video konferans görüşme kalitesini olumsuz etkilememiştir. VPN bağlantısı, uçtan uca güvenli bir bağlantı kurmak için paketleri şifreler ve paketlere ek başlıklar ekler. Paketlere uygulanan bu işlemler paketlerin fazladan gecikmesine sebep olur. Güvenlik duvarı ve VPN kullanımları uçtan uca gecikme süresi yönünden

karşılaştırıldığında ise, VPN kullanımının daha fazla uçtan uca gecikme artışına neden olduğu saptanmıştır. VPN kullanımında güvenlik duvarı üzerindeki paket filtreleme işlemi atlanmakta ve güvenilir olarak tanımlanmış iki uç nokta arasında tüm veri iletişimi sanki aynı yerel alan ağındaymış gibi gerçekleşmektedir. Bu yüzden VPN kullanıldığındaki paket gecikme varyasyon değerleri hiçbir güvenlik çözümü kullanılmadığında elde edilen değerlere eşit çıkmıştır.

Video konferans uygulamalarında WLAN kullanımının uçtan uca gecikme ve gecikme varyasyonu parametrelerini LAN kullanımına göre daha fazla artırdığı bu çalışmanın diğer bir bulgusudur. LAN ve WLAN teknolojileri birçok protokol ve standardı ortak kullanmakla birlikte bazı katmanlarda farklı protokol ve standartlar kullanmaktadırlar. Bu çalışmada LAN'da fiziksel katmanda 802.3 standardı kullanılırken, WLAN'da 802.11g standardı kullanılmıştır. Bu gibi protokol farklılıkları ile WLAN ağlarına özgü yayılma gecikmesi ve AP'ye olan uzaklık gibi parametreler WLAN ağlarındaki paketlerde LAN'daki kullanıma göre daha fazla gecikmeye sebep olmaktadır.

Bu çalışmada ayrıca, video çözünürlüğünün artmasının uçtan uca gecikme süresini ve paket gecikme varyasyonunu artırdığı sonucuna ulaşılmıştır. Paket büyüklüğünün artmasıyla ağ bileşenlerinde gerçekleşen işlem süreleri de artacağından bu durum beklenen bir sonuç olarak değerlendirilir.

5.2. TARTIŞMA ve ÖNERİLER

Bu çalışmada, video konferans uygulamalarında güvenlik duvarı ve VPN kullanımıyla uygulama performansına ait bazı değerlerde artış meydana geldiği tespit edilmiştir. Özellikle video çözünürlüğünün artmasıyla uçtan uca gecikme süresindeki artışın fazlalaştığı değerlendirilirse, çok daha yüksek video çözünürlükleri için güvenlik duvarları ve VPN bağlantılarının daha fazla geliştirilmesi ya da video konferans görüşmeleri için özelleştirilmesi gibi çözümler önerilebilir.

Video konferans uygulamalarını LAN ağlarında kullanmanın WLAN ağlarına göre daha yüksek performans sağladığı çalışmanın diğer bir bulgusudur. Video konferans uygulaması gibi gerçek zamanlı multimedya uygulamaları, uçtan uca gecikme ve gecikme varyasyonu değerlerindeki artışa karşı oldukça duyarlıdır. WLAN teknolojisinde bu artışlara neden olabilecek protokol ve standartlar ile diğer değişkenlerin daha da geliştirilmesi gerektiği açıktır. Özellikle WLAN ağları üzerinden yüksek çözünürlüklü

video konferans görüşmesi gerçekleştirilirken, uygulama performansının düşmesi durumunda LAN kullanımına geçilmesinin daha yerinde olacağı söylenebilir.

Bu çalışmada video konferans uygulama benzetimleri üç katılımcı ve belirli video çözünürlük değerleriyle gerçekleştirilmiştir. Gitgide artan güncel ihtiyaçlar, çok daha fazla katılımcı ve daha yüksek çözünürlük değerleriyle video konferans uygulamalarının gerçekleştirilmesini gerektirmektedir. Katılımcı sayısında ve çözünürlük değerlerindeki artış ağ üzerinden iletilen veri miktarında da artışı doğuracaktır. Bu durum iletilen paket boyutlarını küçültmek için daha gelişmiş video sıkıştırma tekniklerine ve algoritmalarına olan ihtiyacı net bir şekilde ortaya koymaktadır. Yine bu durum, ağ protokollerinin ve bileşenlerinin daha fazla geliştirilmesini zorunlu kılmaktadır.

Bu çalışma, farklı parametreler kullanılarak daha da geliştirilebilir. Bu bağlamda, video konferans uygulamalarında

- Daha yüksek video çözünürlük değerlerinin kullanılması,
- Katılımcı sayısının artırılması,
- Daha farklı ağ teknolojilerinin kullanılması,
- Ağ cihazlarının özelliklerinin artırılması ve
- Farklı kuyruklama ve yönlendirme yöntemlerinin kullanılması

performans etkileri analiz edilecek diğer alanlar olarak sıralanabilir. Bu çalışmanın bu alanlarda ileride yapılacak çalışmalarla birlikte değerlendirilmesi ağ protokollerinin, ağ bileşenlerinin ve video konferans uygulamalarının daha da geliştirilmesi için çok daha anlamlı bilgiler elde edilmesini sağlayacaktır.

6. KAYNAKLAR

[1] D. Taser, E. Aydin, A. O. Torgaloz, ve Y. Rofcanin, "An examination of remote e-working and flow experience: The role of technostress and loneliness", *Computers in Human Behavior*, c. 127, Şub. 2022.

[2] I. B. A. I. Iswara, I. G. M. N. Desnanjaya, I. B. G. Sarasvananda, I. G. Adnyana, ve I. D. P. G. W. Putra, "Analysis of Quality of Service (QoS) Apache Open Meeting Video Conference Application and Bigbluebutton on Virtual Private Server", *2021 6th International Conference on New Media Studies, CONMEDIA 2021*. ss. 1-6, 2021.

[3] N. Austin, R. Hampel, ve A. Kukulska-Hulme, "Video conferencing and multimodal expression of voice: Children's conversations using Skype for second language development in a telecollaborative setting", *System*, c. 64, ss. 87-103, Şub. 2017.

[4] K. Okabe-Miyamoto, E. Durnell, R. T. Howell, ve M. Zizi, "Video conferencing during emergency distance learning impacted student emotions during COVID-19", *Computers in Human Behavior Reports*, c. 7, Ağu. 2022.

[5] R. S. Oeppen, G. Shaw, ve P. A. Brennan, "Human factors recognition at virtual meetings and video conferencing: how to get the best performance from yourself and others", *British Journal of Oral and Maxillofacial Surgery*, c. 58, sy 6. 2020. doi: 10.1016/j.bjoms.2020.04.046.

[6] L. Billingsley, "Using Video Conferencing Applications to Share the Death Experience During the COVID-19 Pandemic", *J Radiol Nurs*, c. 39, sy 4, ss. 275-277, Ara. 2020.

[7] L. Liu, J. Li, H. Xu, K. Xue, ve J. C. Xue, "Efficient Real-time Video Conferencing with Adaptive Frame Delivery", *Computer Networks*, c. 234, sy 10, Eki. 2023, doi: 10.1016/j.comnet.2023.109918.

[8] A. M. Suduc ve M. Bizoi, "AI shapes the future of web conferencing platforms", içinde *Procedia Computer Science*, Elsevier B.V., 2022, ss. 288-294. doi: 10.1016/j.procs.2022.11.177.

[9] A. C. M. Queiroz, A. Y. Lee, M. Luo, G. Fauville, J. T. Hancock, ve J. N. Bailenson, "Too tired to connect: Understanding the associations between video-conferencing, social connection and well-being through the lens of zoom fatigue", *Comput Human Behav*, c. 149, Ara. 2023, doi: 10.1016/j.chb.2023.107968.

[10] M. Baldi ve Y. Ofek, "End-to-End Delay Analysis of Videoconferencing over Packet-Switched Networks", *IEEE/ACM Transactions on Networking*, c. 8, sy 4, ss. 479-492, 2000.

[11] Scott. Firestone, Thiya. Ramalingam, ve Steve. Fry, *Voice and video conferencing fundamentals*. Cisco Press, 2007.

[12] F. A. Sofian, "Dramatism of A Video Conferencing Class: Student's Behavior and Expectations", içinde *Proceedings of the 2023 17th International Conference on Ubiquitous Information Management and Communication, IMCOM 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/IMCOM56909.2023.10035622.

[13] P. Gladović, N. Deretić, ve D. Drašković, "Video Conferencing and its Application in Education", *JTTTP - JOURNAL OF TRAFFIC AND TRANSPORT THEORY AND PRACTICE*, c. 5, sy 1, Mar. 2020, doi: 10.7251/jtttp2001045g.

[14] T. P. Van, C. N. T. Xuan, ve H. P. Minh, "SunFA - An open-source application for behavior analysis in online video-conferencing", içinde *Proceedings - 2022 RIVF International Conference on Computing and Communication Technologies, RIVF 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, ss. 578-583. doi: 10.1109/RIVF55975.2022.10013871.

[15] M. Humayun Kabir, S. Islam, M. Javed Hossain, ve S. Hossain, "Detail Comparison of Network Simulators", *Int J Sci Eng Res*, c. 5, sy 10, 2014, [Çevrimiçi]. Erişim adresi: http://www.ijser.org

[16] E. Weingartner, H. vom Lehn, ve K. Wehrle, "A performance comparison of recent network simulators", içinde *2009 IEEE International Conference on Communications*, IEEE, 2009, ss. 1-5. doi: 10.1109/ICC.2009.5198657.

[17] S. Afzal, V. Testoni, C. E. Rothenberg, P. Kolan, ve I. Bouazizi, "A holistic survey of multipath wireless video streaming", *Journal of Network and Computer Applications*, c. 212, Mar. 2023, doi: 10.1016/j.jnca.2022.103581.

[18] F. Tommasi, V. De Luca, ve C. Melle, "Packet losses and objective video quality metrics in H.264 video streaming", *J Vis Commun Image Represent*, c. 27, ss. 7-

27, 2015, doi: 10.1016/j.jvcir.2014.12.003.

[19] Y. Bai, Y. Chu, ve M. R. Ito, “Dynamic end-to-end QoS Support for Video Over the Internet”, *AEU - International Journal of Electronics and Communications*, c. 65, sy 5, ss. 385-391, May. 2011, doi: 10.1016/j.aeue.2010.07.002.

[20] S. Liu, S. P. Lee, K. H. Kim, Z. Zhang, ve K. W. Rim, “Achieving high-level QoS in multi-party video-conferencing systems via exploitation of global time”, içinde *Proceedings of the 2009 IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing, ISORC 2009*, IEEE Computer Society, 2009, ss. 151-160. doi: 10.1109/ISORC.2009.51.

[21] M. Baldi ve Y. Ofek, “End-to-end Delay of Videoconferencing over Packet Switched Networks”, içinde *IEEE INFOCOM ’98, the Conference on Computer Communications. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies.*, 1998, ss. 1084-1092.

[22] A. L. H. Chow, H. Yang, C. H. Xia, M. Kim, Z. Liu, ve H. Lei, “EMS: Encoded Multipath Streaming for Real-time Live Streaming Applications”. IEEE, 2009. Erişim: 21 Mart 2024. [Çevrimiçi]. Erişim adresi: https://ieeexplore.ieee.org/document/5339681

[23] R. Steinmetz, “Human Perception of Jitter and Media Synchronization”, *IIEEE Journal on Selected Areas in Communications*, c. 14, sy 1, ss. 61-72, 1996.

[24] A. Vakili ve J. C. Grégoire, “QoE management for video conferencing applications”, *Computer Networks*, c. 57, sy 7, ss. 1726-1738, May. 2013, doi: 10.1016/j.comnet.2013.03.002.

[25] B. Reddy Bhimireddy, A. Nimmagadda, H. Kurapati, L. Reddy Gogula, R. Rani Chintala, ve V. Chandra Jadala, “Web Security and Web Application Security: Attacks and Prevention”, içinde *2023 9th International Conference on Advanced Computing and Communication Systems, ICACCS 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, ss. 2095-2099. doi: 10.1109/ICACCS57279.2023.10112741.

[26] M. G. Gouda ve A. X. Liu, “Structured firewall design”, *Computer Networks*, c. 51, sy 4, ss. 1106-1120, Mar. 2007, doi: 10.1016/j.comnet.2006.06.015.

[27] A. Korty, D. Calarco, ve M. Spencer, “Balancing risk with virtual private networking during a pandemic”, *Bus Horiz*, c. 64, sy 6, ss. 757-761, Kas. 2021, doi: 10.1016/j.bushor.2021.07.011.

[28] L. Das Dhomeja, S. Abbasi, A. A. Shaikh, ve Y. A. Malkani, "Performance Analysis of WLAN Standards for Video Conferencing Applications", *International Journal of Wireless & Mobile Networks*, c. 3, sy 6, ss. 59-69, Ara. 2011, doi: 10.5121/ijwmn.2011.3605.

[29] M. I. Mohamed Abouseda, K. A. Bozed, ve A. Ragab Zerek, "Simulation of Video Conferencing over IP Network with QoS Using Riverbed", içinde *2nd International Conference on Automation, Control, Engineering and Computer Science (ACECS-2015)*, 2015.

[30] K. Sharma, N. Bhatia, ve N. Kapoor, "Performance Evaluation of 802.11 WLAN Scenarios in OPNET Modeler", *Int J Comput Appl*, c. 22, sy 9, May. 2011.

[31] P. Singh, "Evaluation of Various Traffic Loads in MANET with DSR Routing Protocol Through Use of OPNET Simulator", *International Journal of Distributed and Parallel systems*, c. 3, sy 3, ss. 75-83, May. 2012, doi: 10.5121/ijdps.2012.3308.

[32] H. A. Mohammed ve A. Hussein Ali, "Effect of Some Security Mechanisms on the QoS VoIP Application Using OPNET", *International Journal of Current Engineering and Technology*, c. 3, sy 5, ss. 1626-1630, 2013, [Çevrimiçi]. Erişim adresi: http://inpressco.com/category/ijcet

[33] M. K. Hasan, "Farklı Ağ Teknolojilerinde Trafik Ölçümü ve Performans Karşılaştırması", Yüksek Lisans Tezi, Erciyes Üniversitesi, Kayseri, 2017.

[34] M. Aamir, M. Zaidi, ve H. Mansoor, "Performance Analysis of DiffServ based Quality of Service in a Multimedia Wired Network and VPN effect using OPNET", *International Journal of Computer Science Issues*, c. 9, sy 3, ss. 368-376, Haz. 2012.

[35] M. Jacobi ve L. Maycock, "Comparison of IPv4 and IPv6 QoS Implementations Using Differentiated Services". [Çevrimiçi]. Erişim adresi: http://shura.shu.ac.uk/21615/

[36] C. Çakir, H. Kaptan, M. Ü. Teknik, E. Fakültesi, E. Bilgisayar, ve E. Bölümü, "VoIP Teknolojilerinde Opnet Tabanlı Güvenlik Uygulaması", *Bilişim Teknolojileri Dergisi*, c. 2, sy 3, ss. 1-7, 2009.

[37] S. Çam, "Güvenlik Duvarı ve Sanal Özel Ağ Çözümlerinin Ağ Performansına Etkilerinin İncelenmesi", Yüksek Lisans Tezi, Trakya Üniversitesi, Edirne, 2020.

[38] M. C. Güleryüz, "Kablosuz Ağ Standartlarının Karşılaştırılması", Yüksek Lisans Tezi, Yüzüncü Yıl Üniversitesi, Van, 2016.

[39] J. Helkey, L. Holder, ve B. Shirazi, "Comparison of simulators for assessing the ability to sustain wireless sensor networks using dynamic network reconfiguration", *Sustainable Computing: Informatics and Systems*, c. 9, ss. 1-7, Mar. 2016, doi: 10.1016/j.suscom.2016.01.003.

[40] J. Gomez, E. F. Kfoury, J. Crichigno, ve G. Srivastava, "A survey on network simulators, emulators, and testbeds used for research and education", *Computer Networks*, c. 237, Ara. 2023, doi: 10.1016/j.comnet.2023.110054.

[41] W. JRana, "Performance Analysis of RIP and OSPF in Network Using OPNET", 2013. [Çevrimiçi]. Erişim adresi: www.IJCSI.org

[42] Manpreet ve J. Malhotra, "A Survey on MANET Simulation Tools", içinde *International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with their Impact on Humanity (CIPECH14)*, 2014, ss. 495-498.

[43] G. H. Adday, S. K. Subramaniam, Z. A. Zukarnain, ve N. Samian, "Investigating and Analyzing Simulation Tools of Wireless Sensor Networks: A Comprehensive Survey", *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3362889.

[44] A. ur R. Khan, S. M. Bilal, ve M. Othman, "A Performance Comparison of Network Simulators for Wireless Networks", *International Journal of Computer Science Issues*, Tem. 2013.

[45] T. Arvind, "A Comparative Study of Various Network Simulation Tools", *International Journal of Computer Science & Engineering Technology (IJCSET)*, c. 7, sy 8, ss. 374-378, Ağu. 2016.

[46] G. Carneiro, P. Fortuna, ve M. Ricardo, "FlowMonitor - a network monitoring framework for the Network Simulator 3 (NS-3)". *ICST (Institute for Computer* Sciences, Social-Informatics and Telecommunications Engineering), s. 628, 2009.

[47] A. Varga ve R. Hornig, "An overview of the OMNeT++ simulation environment", içinde *1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems and Workshops*, Mar. 2008, ss. 1-10. doi: 10.1145/1416222.1416290.

[48] A. Musa ve I. Awan, “Functional and Performance Analysis of Discrete Event Network Simulation Tools”, *Simulation Modelling Practice and Theory*, c. 116. Elsevier B.V., 01 Nisan 2022. doi: 10.1016/j.simpat.2021.102470.

[49] Zheng. Lu ve Hongji. Yang, *Unlocking the Power of OPNET Modeler*. Cambridge University Press, 2012.

[50] A. S. Sethi ve V. Y. Hnatyshin, *The Practical OPNET User Guide for Computer Network Simulation*. Chapman & Hall/CRC, 2012.

[51] S. Mittal, “OPNET: An Integrated Design Paradigm for Simulations”, *Software Engineering : An International Journal (SEIJ)*, c. 2, sy 2, ss. 57-67, Eyl. 2012, [Çevrimiçi]. Erişim adresi: https://hal.science/hal-01108526

[52] J. Mohorko, F. Matjaž, ve K. Saša, “Advanced Modelling and Simulation Methods for Communication Networks”, *Microwave Review*, ss. 41-46, Eyl. 2008.

[53] X. Chang, “Network Simulations With OPNET”, içinde *WSC’99. 1999 Winter Simulation Conference Proceedings. “Simulation - A Bridge to the Future” (Cat. No.99CH37038)*, 1999, ss. 307-314. doi: 10.1109/WSC.1999.823089.

[54] E. Kocabaş, “IPv4 ve IPv6 Desteklenen Yönlendirme Protokollerinin Performans Analizi / Karşılaştırılması”, Yüksek Lisans Tezi, Karabük Üniversitesi, Karabük, 2019.

[55] H. Develi, “Süleyman Demirel Üniversitesi Kampüs Ağının OPNET ile Modellenmesi”, Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Isparta, 2009.

[56] A. Ghulam, “Kablosuz Örgü Ağlarında Yönlendirme Protokollerinin Karşılaştırılması”, Yüksek Lisans Tezi, Erciyes Üniversitesi, Kayseri, 2018.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Serdar ARPACI

Yabancı Dili : İngilizce

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Y. Lisans	Bilgisayar Müh.	Düzce Üniversitesi	2024
Lisans	Bilgisayar Müh.	Hacettepe Üniversitesi	2003
Lise	Sayısal	Gazi Anadolu Lisesi	1994

TEZDEN ÇIKAN YAYIN

S. Arpacı ve A. Şentürk, "Performance Analysis of Firewall and Virtual Private Network (VPN) Usage in Video Conferencing Applications," *Düzce University Journal of Science & Technology*, (Basım Aşamasında).