Düzce University Journal of Science & Technology, 12 (2024) 1879-1894

Düzce University
Journal of Science & Technology

Research Article

Performance Analysis of Firewall and Virtual Private Network (VPN) Usage in Video Conferencing Applications

Serdar ARPACI [a,*], Arafat ŞENTÜRK [b]

[a] *Department of Computer Technologies, Akçakoca Vocational School, Düzce University, Düzce, TURKEY*
[b] *Department of Computer Engineering, Faculty of ENGINEERING, Düzce University, Düzce, TURKEY*
* *Corresponding author's e-mail address: serdararpaci@duzce.edu.tr*
DOI: 10.29130/dubited.1462133

ABSTRACT

Rapid 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 improvements in video conferencing applications, which enable users in different locations at the same time to communicate via video and audio over internet. 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. VPN, on the other hand, provides a secure point-to-point connection to a corporate network through the internet cloud. In this study, the effects of firewall and VPN usage in video conferencing applications were analyzed in terms of application performance. In video conferencing applications; since there is a real-time, bidirectional and large-scale data flow between the participants, delay and packet loss determine the performance of these applications. Analyzing how these applications perform when used with firewalls and VPN will guide further improvements in network protocols, components and related applications. In the study in which the simulation method was used, the data obtained from the simulation of different scenarios created with the OPNET tool were analyzed comparatively.

Keywords: *Network Performance, OPNET, Video Conferencing*

Video Konferans Uygulamalarında Güvenlik Duvarı ve Sanal Özel Ağ (VPN) Kullanımının Performans Analizi

ÖZ

Bilgi ve iletişim teknolojilerindeki süratli gelişmeler; 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; aynı anda farklı yerlerde bulunan kişilerin, internet üzerinden görüntülü ve sesli bir şekilde iletişim kurmalarını sağlayan video konferans uygulamalarında zorunlu gelişmelere yol açmıştır. 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,

Received: 31/03/2024, Revised: 05/04/2024, Accepted: 18/05/2024

kurumsal bir ağ ile internet bulutu arasına konumlandırılarak ağa gelen ve giden trafiği tanımlı kurallara göre filtreleyen cihazdır. Sanal özel ağ ise, kurumsal bir ağa, internet bulutu üzerinden noktadan noktaya güvenli bir bağlantı sağlar. Bu çalışmada, video konferans uygulamalarının güvenlik duvarı ve sanal özel ağ ile kullanımının uygulama performansına etkileri analiz edilmiştir. Video konferans uygulamalarında; katılımcılar arasında gerçek zamanlı, çift yönlü ve büyük boyutlu bir veri akışı olduğundan bu uygulamaların performansında gecikme ve paket kayıpları belirleyici olmaktadır. Bu uygulamaların güvenlik duvarı ve sanal özel ağ ile kullanımının performans analizinin yapılması ağ protokollerinde, ağ bileşenlerinde ve video konferans uygulamalarında daha sonra yapılabilecek iyileştirmeler için yol gösterici olacaktır. Benzetim metodunun kullanıldığı çalışmada, OPNET benzetim aracı ile oluşturulan farklı senaryoların benzetimiyle elde edilen veriler karşılaştırılmalı olarak analiz edilmiştir.

Anahtar Kelimeler: *Ağ Performansı, OPNET, Video Konferans*

I. INTRODUCTION

The developments in information technologies and the decrease in internet usage costs have led transactions and processes using these technologies to become increasingly widespread. In this period; opportunities for fast and easy access to information and resources have emerged, business and decision-making processes have become possible through services and applications provided over the internet, and many applications that institutions and businesses offer to citizens over the internet have emerged. Remote working opportunities have emerged for employees, and institutions and businesses have transitioned to flexible working models by transcending geographical borders [1], [2]. Learning opportunities have been expanded with online education applications in educational institutions [3], [4]. Especially the global Covid-19 pandemic period has caused mandatory developments in application areas such as e-learning and e-meeting, the infrastructure of which is formed by video conferencing technology [4], [5], [6], [7].

Video conferencing is a communication technology that enables people who are in different places at the same time to communicate with each other via audio and video over an internet connection [8], [9]. This technology allows participants to interact using various features such as audio, video, and screen sharing [10], [11]. Video conferencing is generally used for business meetings, distance education, teleworking and personal meetings [12]. This technology can be used in audio and video calls with the participation of a few people, as well as in audio and video calls with dozens of participants [11].

In video conferencing calls, there is a real-time and bidirectional communication between the participants making and answering the call [13]. In this communication, there is a continuous and large data flow. For a quality video conference call, end-to-end delay and delay variation values should be minimized and packet losses should be prevented [13], [14]. End-to-end delay is the time it takes for a packet to arrive at the application layer of the destination from the source [13], [15]. In a video conferencing call, the end-to-end delay should be below human perception so that participants can interact naturally [9], [16]. This value is approximately 100 msecs [9], [16]. However, some studies such as [13], [17] claim that the maximum end-to-end delay for a quality video call is 150 msecs. Delay variation, also referred to as jitter, is defined as the maximum difference between the end-to-end delays of two consecutive packets [18]. Real-time applications such as video conferencing are highly sensitive to delay variation. In a video conferencing call, high delay variation reduces the quality of the call and degrades the user experience by preventing audio and video from synchronizing. The acceptable value for delay variation is 50 msecs at most [15]. Preventing packet loss in video conferencing calls is of vital importance for call quality [19]. In this context, the packet loss rate value, which determines the quality of the call, can be at most 1% [17]. Otherwise, the call quality is noticeably degraded. The most popular video conferencing applications used today are Zoom, Google Meet, Microsoft Teams and Skype [11], [20].

Technological developments causing the rapid increase in applications served over internet are also causing a significant increase in the number of devices connected to internet and in the traffic flowing over internet. As a result, the security needs of applications used over internet, such as video conferencing applications, are growing in proportion to the increasing risks of security threats [21]. The use of a firewall and VPN are the most basic security solutions for applications used over the internet, such as video conferencing applications. A firewall is a device that is placed at the internet connection point of a corporate network and filters the network traffic passing through it according to defined rules [22]. A VPN, on the other hand, allows a node outside the network to establish a secure connection to a corporate network through the internet cloud [23]

This study investigates the effects of firewall and VPN usage on application performance in video conferencing applications. Using simulation methodology, the study compares and analyses the results obtained by executing different simulation scenarios. Analysis of the effects of firewall and VPN usage on video conferencing application performance will provide guidance for future improvements in related applications, network protocols and components.

II. RELATED STUDIES

In this section, a literature review is presented. First, studies related to videoconferencing applications were mentioned. Then studies related to VoIP (Voice over Internet Protocol), another delay sensitive real-time application, were presented. Later, other network performance studies were given. All the studies presented in this section used the simulation method. Finally, the contribution of this study to the literature is mentioned.

In the study [24], the effects of using 802.11a, 802.11b and 802.11g standards in video conferencing applications are analyzed in terms of application performance. In the study where the simulation method was used, a different scenario was created for each standard. During the simulations of the scenarios, end-to-end delay time, WLAN (Wireless Local Area Network) delay time, MAC (Medium Access Control) delay time, number of packets sent, number of packets received, load and throughput statistical data were collected. When the results were analyzed, it was stated that video conferencing applications performed best in 802.11a standard and worst in 802.11b standard.

The study [25] analyzed the effects of FIFO (First-In-First-Out) queuing and WFQ (Weighted-Fair Queuing) mechanisms on the performance of video conferencing applications. During the simulations of the scenarios, data such as end-to-end delay time, packet delay variation, number of packets sent and received were collected and compared. As a result of the study, it was concluded that in terms of application performance, both queuing mechanisms provide results within acceptable value ranges, however, the FIFO queuing mechanism provides a better result.

In the study [26], the use of HTTP (HyperText Transfer Protocol), Remote Login, video conferencing and VoIP applications in 802.11 standard was analyzed in terms of performance. During the simulation of the scenarios, the number of packets sent and WLAN throughput statistics were collected and analyzed. Although the number of nodes was higher in HTTP and Remote Login applications, the data flow was lower compared to video conferencing and VoIP applications. As a result of the study, it was concluded that video conferencing and VoIP applications are prioritized in the network since they are delay-sensitive and real-time applications.

The study [27] analyzed the performance of DSR (Dynamic Source Routing) routing protocol under different traffic loads. HTTP, FTP (File Transfer Protocol), e-mail and video conferencing applications were used in the simulation scenarios. End-to-end delay time and throughput values were used as performance evaluation criteria. According to the simulation results, the average end-to-end delay time was the highest in the video conferencing application and the lowest in the HTTP application. In terms of throughput, video conferencing application achieved the highest value while HTTP application achieved the lowest value. According to the overall results, it is concluded that HTTP application performed the best with DSR routing algorithm.

In the study [28], the performance of VoIP application with firewall and VPN was analyzed. During the simulation of the scenarios, end-to-end delay time, packet delay variation, number of sent and received packets values were collected. By analyzing the data, it has been stated that the use of VPN in VoIP applications gives better results than the use of firewall.

The study [29] compared the performance of MPLS (Multiprotocol Label Switching) and IP (Internet Protocol) routing algorithms using HTTP, FTP, VoIP and video conferencing applications. Data such as HTTP page response time, amount of data sent and received, packet delay variation and IP packet losses were collected during the simulation of the scenarios. As a result of the study, it was stated that MPLS routing performs better than IP routing.

In the study [30], the performance of FTP, database, VoIP and video conferencing applications were compared using Priority Queuing (PQ) and Weighted Fair Queuing (WFQ) mechanisms. Statistical data such as queuing delay time, queuing delay variation, end-to-end delay time, buffer memory usage, average throughput were collected during the execution of the simulated scenarios. According to the results, the video conferencing application produced the highest queuing delay time and queuing delay variation values in both PQ and WFQ mechanisms. As a result of the study; it was found that increasing the amount of buffer memory in the video conferencing applications increases the buffer memory usage while decreasing the dropped traffic, and also increasing the amount of buffer memory decreases the packet delay variation.

In the study [31], the performance of VoIP, a real-time application, was analyzed for its use with Differentiated Services in IPv4 and IPv6 networks. End-to-end delay time, packet delay variation and packet loss values were used as performance evaluation criteria. As a result of the simulations of the scenarios, it was observed that the use of Differentiated Services significantly improves the application performance in both IPv4 and IPv6 networks.

The study [32], investigates the effects of using firewall and VLAN (Virtual Local Area Network) for VoIP applications. According to the simulation results, the use of a firewall prevents threats from the external network, but in the event of an intense attack, performance is degraded, although application accessibility is preserved. While the use of firewall cannot protect against threats from the internal network, the use of a VLAN can. The use of a VLAN also enables the system to run more efficiently.

In the study [33], the effects of firewall and VPN usage on network performance were analyzed. Analyzing the results of simulated scenarios for HTTP, email and database applications, it was found that using a firewall increased application response time, reduced network utilization and the amount of data received. Using a VPN increased application response times more than using a firewall, but reduced network utilization and the amount of data received more than using a firewall.

Our study analyzed the effects of firewall and VPN usage on application performance in video conferencing applications. The end-to-end delay time, delay variation and packet loss values were used as determining criteria for application performance metrics. In our study, where the simulation method was used, statistical data for the corresponding criteria were collected during the simulation of the modelled scenarios. Previous studies have analyzed the performance of applications such as HTTP, FTP, email, database, VoIP and video conferencing in many aspects. However, there is no study specifically on the effects of firewall and VPN usage on application performance in video conferencing applications. This study addresses this gap in the literature by identifying and analyzing the effects of firewall and VPN usage on the performance of video conferencing applications. Future improvements in video conferencing applications, network protocols and components will be based on the identification and analysis of these effects.

III. MATERIAL AND METHOD

This section first introduced the network simulation approach and provided information on the network simulation tool used. It then discusses the network topology and scenarios that were modelled to obtain the study data. Finally, the video conferencing parameters used and the statistical data collected are described.

A. NETWORK SIMULATION and OPNET TOOL

Network simulation is a widely used approach for the design, implementation, optimization and performance evaluation of network topologies by modelling the behavior of a real network operating under various configurations [34]. With this approach, the planned scenarios can be run in a controlled and repetitive manner without the cost of setting up a real test network with real nodes, links and devices [34]. There are various simulation tools used for network simulation. With these tools, complex network topologies and traffic patterns that are difficult or impossible to replicate in a physical network can be easily created [35]. These tools provide the opportunity to test different protocols, compare different network designs and identify potential problems before building a real network. NS-2, NS-3, OMNeT++ and OPNET are among the most popular simulation tools accepted in the literature [35], [36], [37]. [38], [39] are among the studies in which these simulation tools are used. Because OPNET has a high-level graphical interface that is very easy to use [40], [41] and has fast simulation capabilities [41], [42], it was preferred in this study.

OPNET (OPtimized Network Engineering Tool) [43] is a well-recognized simulation tool in the literature that provides a comprehensive development environment for simulating, measuring and evaluating the performance of networks [35]. The main difference that distinguishes OPNET from other network simulation tools is its power and versatility [40]. OPNET, which has three basic functions as modelling, simulation and analysis, includes an extremely well-designed, user-friendly graphical interface [40].

OPNET can be used to design a wide variety of network models such as LAN (Local Area Network), WAN (Wide Area Network), internet network, mobile network, sensor network and satellite network [43]. For a designed network model, different scenarios can be created based on different topologies, routing, traffic and load parameters. These scenarios can be simulated and many different statistical data can be collected.

In the OPNET simulation tool, HTTP, FTP, Email, Database, Print, Remote Login, Video conferencing and VoIP applications are defined as default applications. In this study, the simulation of video conferencing applications was performed with version 14.5 of the OPNET simulation tool.

B. MODELLED TOPOLOGY AND SCENARIOS

The topology modelled in this study is shown in Figure 1. In this topology, a video conferencing call with three participants takes place. In the right part of the topology: two video conferencing clients (Video_Client_1 and Video_Client_2) are located in a local area network and connected to a switch (Switch_Client) via a 100 Mbps network cable. This switch is connected to the router (Router_Client) via a 100 Mbps network cable. In the left part of the topology, a video conferencing server (Video_Server) is located in a corporate network and is connected to a switch (Switch_Server) via a network cable with a speed of 100 Mbps. This switch is connected to a router (Router_Server) via a 100 Mbps network cable. The routers in both parts are connected to the internet cloud (IP Cloud) via fiber cables with a speed of 1 Gbps.

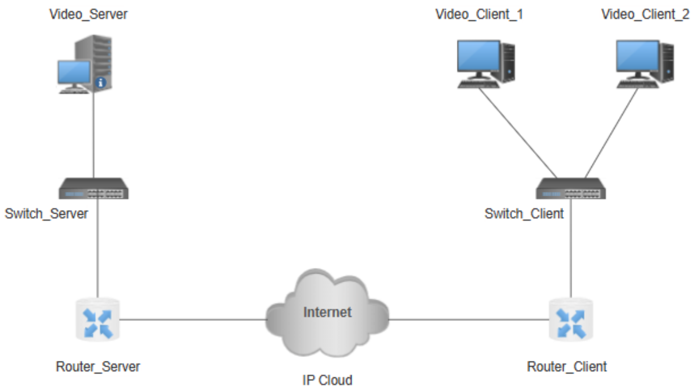


Figure 1. *Video conferencing topology*

Three scenarios were created on this topology. In the first scenario, no firewall and VPN connection were used. In this scenario, the simulation was performed with the topology as shown in Figure 1. This scenario is labelled as LAN in OPNET.
The difference of the second scenario, labelled as LAN_FW in the OPNET tool, from the first scenario is the firewall added to the topology. In this scenario, a firewall object was added between the router (Router_Server) and internet cloud (IP Cloud) objects in the left part of the topology. The topology of the scenario is shown in Figure 2.

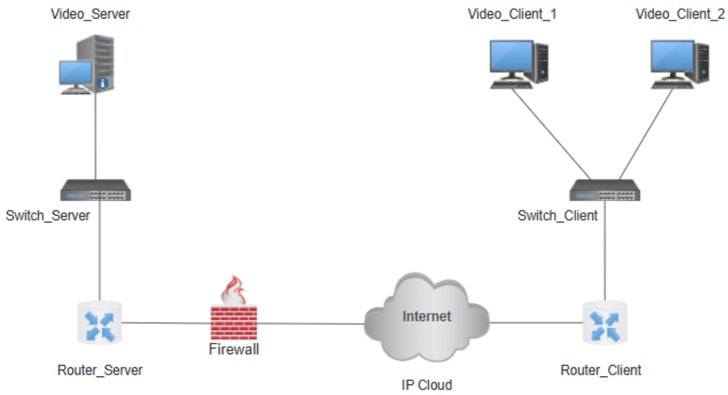


Figure 2. *LAN_FW: Topology of -firewall usage scenario*

The third scenario was created by adding an IP VPN configuration object labelled as VPN to the topology of the second scenario. Firewall and VPN objects were configured to ensure video conferencing traffic is over the VPN connection. The topology of this scenario, labelled as LAN_VPN in OPNET, is shown in Figure 3.

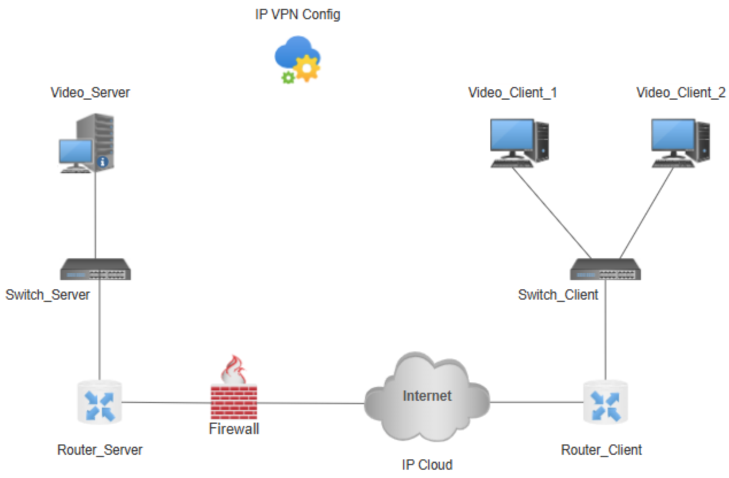


Figure 3. *LAN_VPN: Topology of VPN usage scenario*

C. VIDEO CONFERENCING CALL PARAMETERS

The OPNET simulation tool allows customizing the settings of defined applications. The video packet size of the video conference calls used in this study is 1,440 bytes. In the conference call, 15 video frames are produced every second and transmitted over the network.

D. COLLECTED STATISTICAL DATA

In this study, end-to-end delay, delay variation and packet loss values, which are determinants of the quality of video conferencing calls [13], [14], were measured. In studies such as [24], [25], performance analyses were performed by measuring the same values. In OPNET, the statistics selection screen shown in Figure 4 was accessed by clicking Choose Individual Statistics from the DES menu in the Project Editor. The statistical data collected during the simulation of the scenarios in this study are described in Table 1.

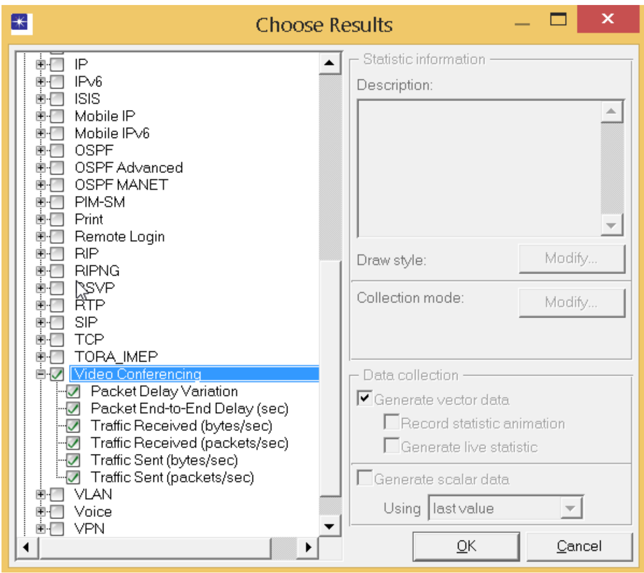


Figure 4. *Statistical data selection screen*

Table 1. Collected statistical data.

Statistics Name	Description	Measurement Unit
Packet End-to-End Delay	End-to-End delay time	msecs
Packet Delay Variation	Delay variation	msecs
Traffic Received	Amount of data received per sec	bytes/sec
Traffic Received	Number of packets received per sec	packets/sec
Traffic Sent	Amount of data sent per sec	bytes/sec
Traffic Sent	Number of packets sent per sec	packets/sec

IV. APPLICATION

In some previous studies, simulation scenarios were executed for 900 seconds in [44], 1,800 seconds in [45], 3,600 seconds in [33], [46]. In this study, on the Manage Scenarios screen of OPNET, which is shown in Figure 5 accessed from the Scenarios menu in the Project Editor, simulation durations are set to 1,800 seconds. By clicking OK, the simulations are executed as shown in the Simulation Execution Manager screen shown in Figure 6. The statistical data collected at the end of the simulation were converted into graphs and the effects of firewall and VPN usage in video conferencing applications on application performance were analyzed.

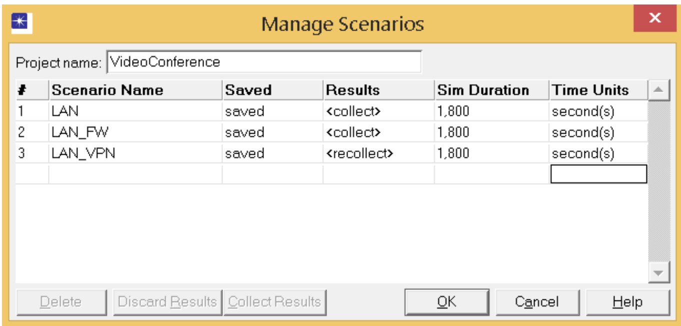


Figure 5. *Manage scenarios screen*

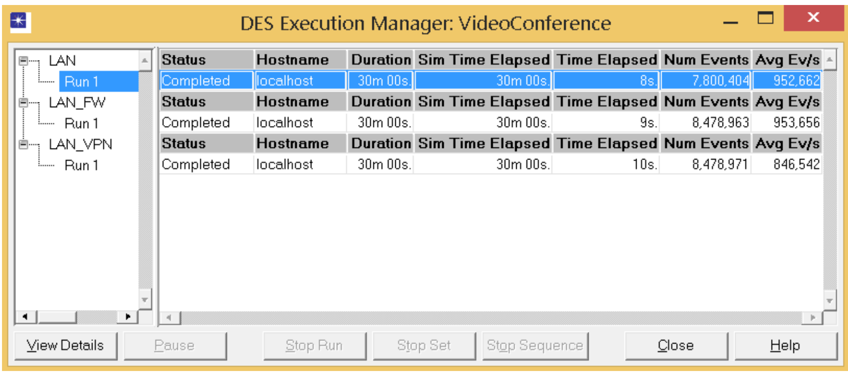


Figure 6. *Simulation execution manager screen*

A. END-TO-END DELAY TIME

As can be seen in Figure.7, the end-to-end delay is 0.54 msecs in the absence of firewall and VPN connection. The use of firewall increases the end-to-end delay by approximately 0.035 msecs. When a VPN connection is used, the end-to-end delay increases by about 0.047 msecs. These found values are below 100 msecs, which is the acceptable value for a quality video conference call.

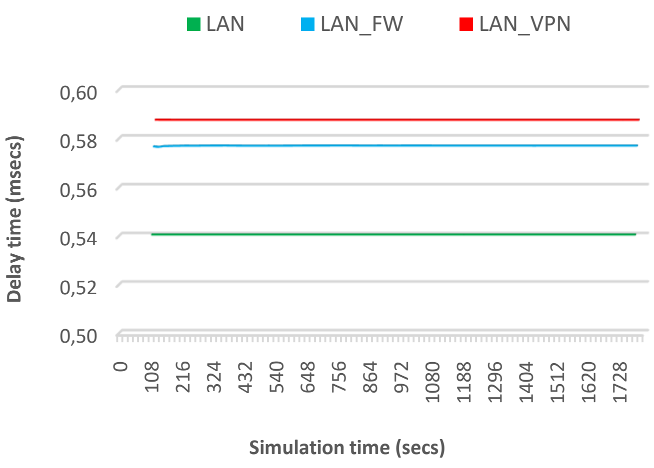


Figure 7. *End-to-end delay time*

B. PACKET DELAY VARIATION (JITTER)

When a firewall and VPN connection are not used, the packet delay variation is 0. In the scenario where a firewall is used, this value is 0.0000012 msecs. When VPN is used, the packet delay variation is again 0. These values are below the acceptable value of 50 msecs for a quality video conference call. The graph of the measured values is shown in Figure.8.

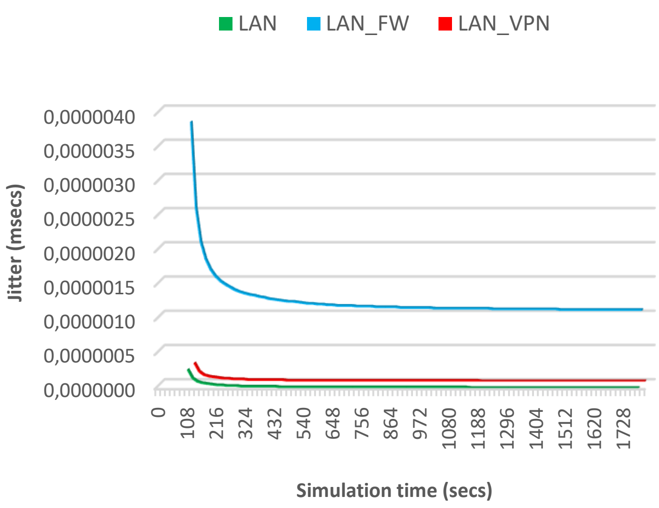
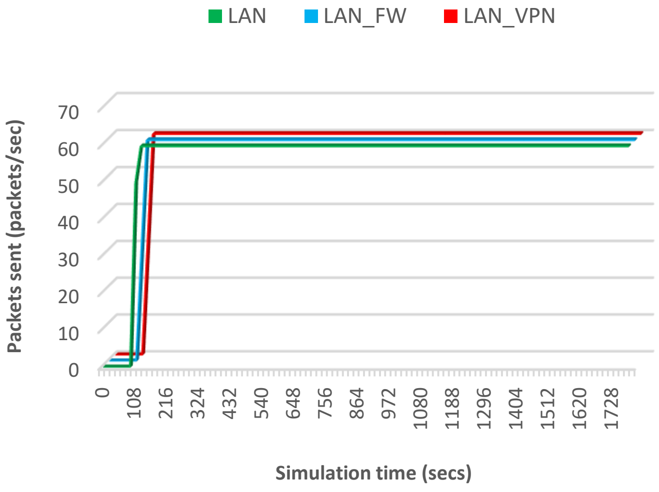


Figure 8. *Packet delay variation (Jitter)*

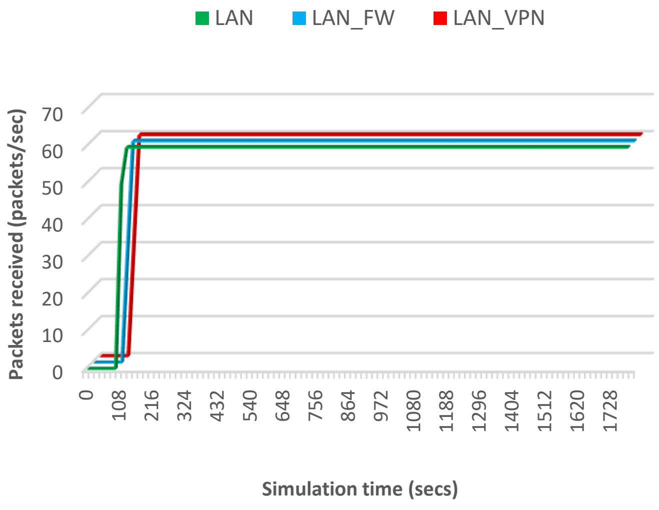
C. NUMBER OF PACKETS SENT AND RECEIVED

The number of packets sent refers to the total number of packets sent by participants in the video conference call per second. The total number of packets sent per second during the video conference call is 60 for all three scenarios, as shown in Figure 9 (a). Each client sends 15 video packets per second. The server sends 30 video packets per second. Therefore, there is no packet loss.

The total number of packets received per second by the participants in the video conference call is 60 for all three scenarios, as shown in Figure 9 (b). Since each client receives 15 video packets per second and the server receives 30 video packets per second, there is no packet loss in the conference call.



(a)



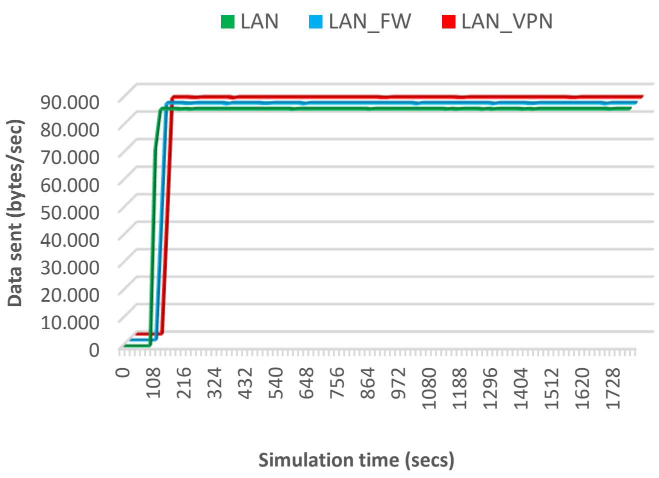
(b)

Figure 9. (a) *Number of packets sent* ***(b)*** *Number of packets received*

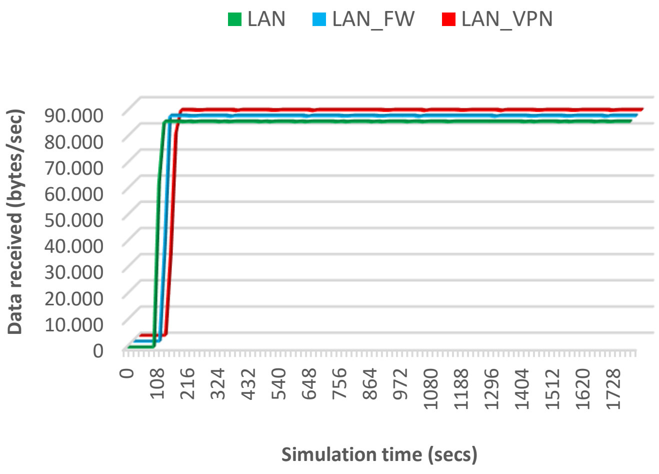
D. AMOUNT OF DATA SENT AND RECEIVED

The amount of data sent is the total amount of data sent by the participants of the call in one second. This value is 86,400 for all scenarios during the video conference call. This value is compatible because 60 video packets of 1,440 bytes each are sent per second across the entire network. The measured values are shown in Figure 10 (a).

The total amount of data received per second by the participants in the video conference call is 86,400 in all scenarios, as shown in Figure 10 (b). In the whole network, a total of 60 video packets of 1,440 bytes each are received per second.



(a)



(b)

Figure 10. (a) *Amount of data sent* ***(b)*** *Amount of data received*

V. CONCLUSION

This section begins by evaluating the results of the study. It then discusses the limitations of the study and how it could be improved. Finally, some suggestions are made for other areas that could be the subject of study.

A. EVALUATION OF THE RESULTS

The use of a firewall and VPN is known to affect the performance of applications used on the network. In this study, their effects on video conferencing applications were measured and analyzed. It was found that the use of a firewall increases the end-to-end delay time by about 0.035 msecs. The firewall filters all packets passing through it according to predefined rules. It allows packets that comply with the rules to pass through while blocking packets that do not comply with the rules. It is clear that this filtering process causes extra delay. When a VPN connection is used, the end-to-end delay time increases by about 0.047 msecs. The VPN connection encrypts packets and adds additional headers to the packets to establish a secure end-to-end connection. These processes applied to the packets cause extra delay. It was also found that the use of a VPN connection causes a greater increase in end-to-end delay time than the use of a firewall.

The study measured packet delay variation as 0 in the scenarios in which no firewall and VPN were used. This indicates that two consecutive packets arrive at the destination with the same latency in these scenarios. When the firewall was used, the packet delay variation was 0.0000012 msecs. While the firewall filters the packets passing through it, it causes a delay in the packets. However, it is almost impossible for two consecutive packets that need to reach their destination at the same time to have the same filtering time. Packet delay variation takes the value 0 when VPN is used. When using a VPN, the filtering process on the firewall is bypassed and all data communication takes place directly between two secure endpoints.

When packet loss is considered in the study, video packets are successfully transmitted in all simulated scenarios and no packet loss is observed.

In this study, end-to-end delay, delay variation and packet loss values were measured for video conferencing calls. All simulated scenarios meet the minimum requirements for these values. In other words, the modelled topology and scenarios provide high quality video conferencing calls.

B. DISCUSSION AND SUGGESTIONS

With the widening of application areas in accordance with current communication needs, the need to use video conferencing applications with more participants and higher video resolution values is increasing. In addition, video conferencing applications are being enhanced each passing day with additional features such as screen sharing and whiteboarding. As a result of these developments in video conferencing applications, it can be predicted that the effects measured in our study will be greater with the use of higher resolution and more participants. Again, as additional features are added to video conferencing applications, it can be predicted that the amount of data transmitted, and thus the effects analyzed in our study, will increase. In this context, the evaluation of our study, together with further studies with higher resolution and more participants, will provide much more meaningful results. Thus, more advance information will be obtained for improvements in video conferencing applications, which is one of our study goals. Based on this information, for example, video compression algorithms and methods can be improved. This advanced information will be used to help improve network protocols and components, one of the goals of our study.

In this study, video conferencing application is studied with a particular video resolution and three participants. Further developments of the study using different parameters, will provide more meaningful information in this area. In this context, in video conferencing applications

- Using higher video resolution values,
- Increasing the number of participants,
- Using different network technologies such as Wi-Fi (Wireless Fidelity) and WiMAX (Worldwide Interoperability for Microwave Access),
- Changing the features of network devices,
- Using different network topologies,
- Using different queuing mechanisms and
- Using different routing methods,

are other areas that need to be analyzed for their effects on performance. Another area worthy of further research is the application of similar studies to web conferencing applications, which are used over web browsers.

VI. REFERENCES

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

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

[3] N. Austin, R. Hampel, and A. Kukulska-Hulme, “Video conferencing and multimodal expression of voice: Children’s conversations using Skype for second language development in a telecollaborative setting,” *System*, vol. 64, pp. 87–103, Feb. 2017.

[4] K. Okabe-Miyamoto, E. Durnell, R. T. Howell, and M. Zizi, “Video conferencing during emergency distance learning impacted student emotions during COVID-19,” *Computers in Human Behavior Reports*, vol. 7, Aug. 2022.

[5] R. S. Oeppen, G. Shaw, and 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*, vol. 58, no. 6, pp. 643–646, Jul. 2020.

[6] L. Billingsley, “Using Video Conferencing Applications to Share the Death Experience During the COVID-19 Pandemic,” *Journal of Radiology Nursing*, vol. 39, no. 4, pp. 275–277, Dec. 2020.

[7] L. Liu, J. Li, H. Xu, K. Xue, and J. C. Xue, “Efficient Real-time Video Conferencing with Adaptive Frame Delivery,” *Computer Networks*, vol. 234, Oct. 2023.

[8] A. C. M. Queiroz, A. Y. Lee, M. Luo, G. Fauville, J. T. Hancock, and J. N. Bailenson, “Too tired to connect: Understanding the associations between video-conferencing, social connection and well-being through the lens of zoom fatigue,” *Computers in Human Behavior*, vol. 149, Dec. 2023.

[9] M. Baldi and Y. Ofek, “End-to-End Delay Analysis of Videoconferencing over Packet-Switched Networks,” *IEEE/ACM Transactions on Networking*, vol. 8, no. 4, pp. 479–492, Aug. 2000.

[10] S. Firestone, T. Ramalingam, and S. Fry, *Voice and Video Conferencing Fundamentals*. Cisco Press, 2007.

[11] F. A. Sofian, “Dramatism of A Video Conferencing Class: Student’s Behavior and Expectations,” *Proceedings of the 2023 17th International Conference on Ubiquitous Information Management and Communication*, pp. 1–5, 2023.

[12] P. Gladović, N. Deretić, and D. Drašković, “Video Conferencing and its Application in Education,” *JTTTP - Journal of Traffic and Transport Theory and Practice*, vol. 5, no. 1, Mar. 2020.

[13] S. Afzal, V. Testoni, C. E. Rothenberg, P. Kolan, and I. Bouazizi, “A holistic survey of multipath wireless video streaming,” *Journal of Network and Computer Applications*, vol. 212, Mar. 2023.

[14] F. Tommasi, V. De Luca, and C. Melle, “Packet losses and objective video quality metrics in H.264 video streaming,” *Journal of Visual Communication and Image Representation*, vol. 27, pp. 7–27, Feb. 2015.

[15] S. Liu, S. P. Lee, K. H. Kim, Z. Zhang, and K. W. Rim, “Achieving high-level QoS in multi-party video-conferencing systems via exploitation of global time,” *Proceedings of the 2009 IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing*, pp. 151–160, 2009.

[16] M. Baldi and Y. Ofek, “End-to-end Delay of Videoconferencing over Packet Switched Networks,” *Proceedings of the Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies*, vol.3, pp. 1084-1092, Jan. 98.

[17] A. L. H. Chow, H. Yang, C. H. Xia, M. Kim, Z. Liu, and H. Lei, “EMS: Encoded Multipath Streaming for Real-time Live Streaming Applications,” *Proceedings of the 17th annual IEEE International Conference on Network Protocols*, pp. 233-243, Oct. 2009

[18] R. Steinmetz, “Human Perception of Jitter and Media Synchronization,” *Journal on Selected Areas in Communications*, vol. 14, no. 1, pp. 61-72, Jan. 1996.

[19] A. Vakili and J. C. Grégoire, “QoE management for video conferencing applications,” *Computer Networks*, vol. 57, no. 7, pp. 1726–1738, May 2013.

[20] T. P. Van, C. N. T. Xuan, and H. P. Minh, “SunFA - An open-source application for behavior analysis in online video-conferencing,” *Proceedings of 2022 RIVF International Conference on Computing and Communication Technologies,* pp. 578–583, 2022.

[21] B. Reddy Bhimireddy, A. Nimmagadda, H. Kurapati, L. Reddy Gogula, R. Rani Chintala, and V. Chandra Jadala, “Web Security and Web Application Security: Attacks and Prevention,” *2023 9th International Conference on Advanced Computing and Communication Systems,* pp. 2095–2099, 2023.

[22] M. G. Gouda and A. X. Liu, “Structured firewall design,” *Computer Networks*, vol. 51, no. 4, pp. 1106–1120, Mar. 2007.

[23] A. Korty, D. Calarco, and M. Spencer, “Balancing risk with virtual private networking during a pandemic,” *Business Horizons*, vol. 64, no. 6, pp. 757–761, Nov. 2021.

[24] L. Das Dhomeja, S. Abbasi, A. A. Shaikh, and Y. A. Malkani, “Performance Analysis of WLAN Standards for Video Conferencing Applications,” *International Journal of Wireless & Mobile Networks,* vol. 3, no. 6, pp. 59–69, Dec. 2011.

[25] M. I. Mohamed Abouseda, K. A. Bozed, and A. Ragab Zerek, “Simulation of Video Conferencing over IP Network with QoS Using Riverbed,” *Proceedings of 2nd International Conference on Automation, Control, Engineering and Computer Science*, 2015.

[26] K. Sharma, N. Bhatia, and N. Kapoor, “Performance Evaluation of 802.11 WLAN Scenarios in OPNET Modeler,” *International Journal of Computer Applications*, vol. 22, no. 9, pp. 30-35, May 2011.

[27] 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*, vol. 3, no. 3, pp. 75–83, May 2012.

[28] H. A. Mohammed, and A. H. Ali, “Effect of Some Security Mechanisms on the QoS VoIP Application Using OPNET,” *International Journal of Current Engineering and Technology*, vol. 3, no. 5, pp. 1626-1630, Dec. 2013.

[29] M. K. Hasan, “Farklı Ağ Teknolojilerinde Trafik Ölçümü ve Performans Karşılaştırması,” M.S. thesis, Dept. Elect. and Electron. Eng., Erciyes Univ., Kayseri, 2017.

[30] M. Aamir, M. Zaidi, and 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*, vol. 9, Jun. 2012.

[31] M. Jacobi, and L. Maycock, “Comparison of IPv4 and IPv6 QoS Implementations Using Differentiated Services.” Accessed: Apr. 22, 2024. [Online]. Available: http://shura.shu.ac.uk/21615/

[32] C. Çakir, and H. Kaptan, “VoIP Teknolojilerinde Opnet Tabanlı Güvenlik Uygulaması,” *Bilişim Teknolojileri Dergisi*, vol. 2, no. 3, Sep. 2009.

[33] S. Çam, “Güvenlik Duvarı ve Sanal Özel Ağ Çözümlerinin Ağ Performansına Etkilerinin İncelenmesi,” M.S. thesis, Dept. Comput. Eng., Trakya Univ., Edirne, 2020.

[34] J. Helkey, L. Holder, and B. Shirazi, “Comparison of simulators for assessing the ability to sustain wireless sensor networks using dynamic network reconfiguration,” *Sustainable Computing: Informatics and Systems*, vol. 9, pp. 1–7, Mar. 2016.

[35] J. Gomez, E. F. Kfoury, J. Crichigno, and G. Srivastava, “A survey on network simulators, emulators, and testbeds used for research and education,” *Computer Networks*, vol. 237, Dec. 2023.

[36] Manpreet, and J. Malhotra, “A Survey on MANET Simulation Tools,” *International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with their Impact on Humanity*, pp. 495-498, Nov. 2014

[37] G. H. Adday, S. K. Subramaniam, Z. A. Zukarnain, and N. Samian, “Investigating and Analyzing Simulation Tools of Wireless Sensor Networks: A Comprehensive Survey,” *IEEE Access*, vol. 12, pp. 22938-22977, 2024.

[38] A. Şentürk, “Kablosuz Multimedya Algılayıcı Ağlar İçin Görüntü Sıkıştırmaya Dayalı Yeni Bir Enerji Duyarlı Uygulama Katmanı Algoritması Geliştirme,” Ph.D. dissertation, Dept. Elect. Electron. and Comput. Eng., Düzce Univ., Düzce, 2017.

[39] A. Senturk, R. Kara, and I. Ozcelik, “Fuzzy logic and image compression based energy efficient application layer algorithm for wireless multimedia sensor networks,” *Computer Science and Information Systems*, vol. 17, no. 2, pp. 509–536, Jun. 2020.

[40] A. Musa and I. Awan, “Functional and Performance Analysis of Discrete Event Network Simulation Tools,” *Simulation Modelling Practice and Theory*, vol. 116., Apr. 2022.

[41] T. Arvind, “A Comparative Study of Various Network Simulation Tools,” International Journal of Computer Science & Engineering Technology, vol. 7, no. 8, pp. 374-378, Aug. 2016.

[42] M. H. Kabir, S. Islam, M. J. Hossain, and S. Hossain, “Detail Comparison of Network Simulators,” *International Journal of Scientific & Engineering Research*, vol. 5, no. 10, pp. 203-218, Oct. 2014.

[43] Z. Lu and H. Yang, Unlocking the Power of OPNET Modeler. Cambridge University Press, 2012.

[44] E. Kocabaş, “IPv4 ve IPv6 Desteklenen Yönlendirme Protokollerinin Performans Analizi / Karşılaştırılması,” M.S. thesis, Dept. Comput. Eng., Karabük Univ., Karabük, 2019.

[45] H. Develi, “Süleyman Demirel Üniversitesi Kampüs Ağının OPNET ile Modellenmesi,” M.S. thesis, Dept. Electron. Comput. Educ., Süleyman Demirel Univ., Isparta, 2009.

[46] A. Ghulam, “Kablosuz Örgü Ağlarında Yönlendirme Protokollerinin Karşılaştırılması,” M.S. thesis, Dept. Comput. Educ., Erciyes Üniversitesi, Kayseri, 2018.