PCMJ

Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

COMPARATIVE ANALYSIS OF VPN NETWORK PERFORMANCE USING MOBILE WI-FI

FARIHA MOHD AZLI
College of Computing, Informatics and Mathematics, Campus Jasin, Jasin, Melaka
2021853872@student.uitm.edu.my

ALYA GEOGIANA BUJA*
College of Computing, Informatics and Mathematics, Campus Jasin, Jasin, Melaka
geogiana@uitm.edu.my

SHAHADAN SAAD
College of Computing, Informatics and Mathematics, Campus Jasin, Jasin, Melaka
shahadan@uitm.edu.my

Article Info

Received: March 2025
Accepted: September 2025
Available Online: November 2025

Abstract

Virtual Private Networks (VPNs) are widely used to enhance online security and privacy, especially when accessing the internet over mobile Wi-Fi networks. However, performance issues emerge from VPN usage because mobile users experience decreased speed alongside greater latency and packet loss which affect activities such as online gaming, streaming and general browsing. This study explores VPN network performance through mobile Wi-Fi connections by evaluating the services from NordVPN, ExpressVPN, and Surfshark. This study has two main objectives which are to conduct a series of experiments to evaluate how VPNs perform under various usage scenarios, including gaming, streaming, and general browsing, and to analyze the performance of network parameters such as speed, latency, and packet loss across different VPN services. Network performance metrics were measured accurately through experiments conducted with Speedtest by Ookla, PingPlotter and Fing as network monitoring tools. The VPN assessment tests executed across three different environments which simulated actual VPN user operations. Data collection showed strong evidence of performance variations between VPN providers because each provider demonstrated unique deficiencies during the different tests. The research findings help VPN users choose VPNs that match their particular needs while generating valuable optimization opportunities for VPN service providers.

Keywords: VPN, Wi-Fi, performance issues, gaming, streaming, general browsing, speed, latency, packet loss.

Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

INTRODUCTION

Online security demands Virtual Private Networks (VPNs) to protect digital activities including regular browsing and streaming videos and playing games online because privacy in this age is crucial. Data encryption alongside secure server traffic redirection protects users from unauthorized access when using VPNs on public and unsecured networks (Ostroukh et al., 2024). The implementation of security features leads to performance decrease in network communications. VPNs create performance problems by reducing network speed and extending latency and causing packet drop which result in worsened user experience. The performance results from using VPNs stem from VPN protocols combined with encryption methods and server location as Abdulazeez et al. explain. Research shows that WireGuard delivers faster and more efficient performances than legacy VPN protocols such as OpenVPN and IPsec because it was introduced in 2019 by Habibovic.

VPN usage continues to expand because people work remotely and want better privacy protection which makes it essential to study their performance characteristics. Research has revealed that while some VPNs excel in low-latency tasks like gaming, others are optimized for high-throughput activities such as streaming and file transfers. These differences arise from factors like server load, routing efficiency, and encryption overhead. Nevertheless, a comprehensive, scenario-based analysis comparing multiple VPN services on real-world metrics such as speed, latency, and packet loss remains scarce. This study aims to bridge this gap by evaluating three popular VPN providers which are NordVPN, ExpressVPN, and Surfshark, using a mobile Wi-Fi network and focusing on common user scenarios to provide actionable insights.

LITERATURE REVIEW

This chapter covered in depth the area consisted in this project. This chapter offers a comprehensive review of the literature on WI-Fi, Virtual Private Network, and network performance.

Wi-Fi

Wi-Fi functions as a wireless networking technology that serves as a fundamental communication component for devices to access internet connections and other electronic devices through wireless connections instead of cables. The Wi-Fi network operates with the protocols defined by IEEE 802.11 that establish wireless local area networks (WLANs). The Wi-Fi technology has undergone substantial development throughout time by releasing new versions that achieve better connection speeds and playing a vital role in security improvements (Ahmad, 2022). The adoption of Wi-Fi as a standard has been made possible due to its easy use together with its versatility that allows multiple applications and connects both homes to enterprise networks and Internet of Things devices. Future digital communication will depend heavily on Wi-Fi because wireless connectivity demand continues increasing (Frascolla et al., 2023).

The necessity of Wi-Fi continues to rise because businesses in healthcare, education and entertainment now heavily depend on wireless connectivity. Wi-Fi adoption surged during the COVID-19 pandemic because remote work and online learning as well as virtual meetings became necessary standards (Reshef & Cordeiro, 2022). The surge in Wi-Fi demands genuine network infrastructures with sufficient bandwidth capacity to fulfill continuously increasing device numbers. Modern digital infrastructure relies on Wi-Fi as an essential component because new technologies have introduced Wi-Fi 6 and Wi-Fi 7 features which enhance performance alongside better efficiency and security (Frascolla et al., 2023; Ramezanpour et al., 2023).

Among the advantages of Wi-Fi there exist security and interference problems which represent major obstacles. The security risks of public Wi-Fi require users to protect themselves with VPNs while enabling encryption (Charan Sahu, 2022). Furthermore, the growing population of Wi-Fi networks in cities continually creates problems with signal cross-connections and network jamming which reduces performance levels. The research community together with industry leaders produce new technological and standardization methods which enhance Wi-Fi network security while improving reliability and efficiency. Experts predict that Wi-Fi will power both 5G and subsequent wireless networks through its continued development. (Gao et al., 2021; Liu et al., 2023).

Virtual Private Network

A Virtual Private Network (VPN) is a critical technology that enables secure communication over public networks by creating an encrypted tunnel between the user and the destination. VPNs are widely used to protect data privacy, enhance security, and bypass geographical restrictions. They are particularly valuable in enterprise networks, where they ensure secure remote access and data integrity (Benefits of Using Open Source VPNs in Enterprise Networks, 2024). The evolution of VPNs has been driven by the need for robust security solutions, especially with the rise of remote work and the increasing prevalence of cyber threats (Crawshaw, 2020). VPNs operate at different layers of the network stack, and their effectiveness depends on the protocols and configurations used, making them adaptable to various use cases and environments. As organizations increasingly rely on cloud services and remote workforces, VPNs have become indispensable tools for maintaining secure and private communication channels. Furthermore, the growing complexity of network infrastructures and the rise of sophisticated cyberattacks have necessitated the development of more advanced VPN technologies, such as WireGuard, which offer improved performance and security (Abdulazeez et al., 2020; Gentile et al., 2022).

The importance of VPNs has grown significantly in recent years due to the increasing reliance on digital communication and the need for secure remote access. With the rise of remote work, especially during the COVID-19 pandemic, VPNs have become essential for enabling employees to securely access corporate networks from home or other remote locations (Haeruddin et al., 2023). This shift has highlighted the need for VPNs that are not only secure but also easy to deploy and manage, particularly for organizations with limited IT resources. Additionally, VPNs are increasingly being used to protect sensitive data transmitted over public Wi-Fi networks, which are often vulnerable to cyberattacks (Charan Sahu, 2022). By encrypting data and masking the user's IP address, VPNs provide an additional layer of security that helps prevent unauthorized access and data breaches. This is particularly important for industries such as healthcare and finance, where the protection of sensitive information is critical (Crawshaw, 2020; Fayoumi et al., 2022).

Moreover, VPNs are not just limited to securing remote access; they also play a crucial role in enabling secure communication between geographically dispersed networks. For example, site-to-site VPNs are commonly used by organizations with multiple branch offices

to create a secure and private network that spans different locations (Santoso et al., 2021). This allows employees at different sites to access shared resources and collaborate securely, without the risk of data interception or unauthorized access. In addition to their use in enterprise networks, VPNs are also being adopted in IoT environments, where they are used to secure communication between devices and protect data transmitted over the internet (Gentile et al., 2022). As the number of connected devices continues to grow, the need for secure and reliable communication channels will only increase, further driving the adoption of VPNs in various industries. Overall, VPNs have become a fundamental tool for ensuring secure and private communication in an increasingly interconnected world (Irsyad & Mulyana, 2023; Ostroukh et al., 2024).

Network Performance

Network performance is critical for ensuring seamless connectivity, efficient data transfer, and optimal user experience in modern communication systems. The rise of remote work and bandwidth-intensive applications, such as video streaming and online gaming, has placed significant demands on network infrastructure. According to Fratel (2020), the surge in remote work during the COVID-19 pandemic increased network traffic, highlighting the need for robust performance monitoring tools. Similarly, Fratel also emphasizes that video streaming, which accounts for a large portion of global internet traffic, requires consistent network performance to avoid buffering and poor user experiences. These trends underscore the importance of effective network performance monitoring and optimization.

Emerging technologies like 5G and IoT have further complicated network performance management. 5G networks promise ultra-low latency and high speeds but require advanced tools to monitor dynamic features like network slicing and beamforming . Meanwhile, the growth of IoT has increased the number of connected devices, straining network infrastructure and necessitating real-time performance monitoring (Fratel, 2020).

Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

METHODOLOGY

This project process involved five key phases. Planning, experimental setup, testing, result and analysis, and documentation. These five stages are important for the success of this project.

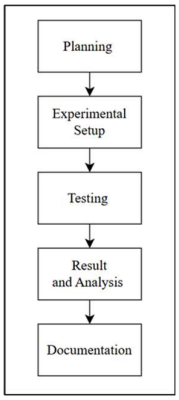

Figure 1: Project Framework

This project examined mobile Wi-Fi network performance from three different VPN service providers. Surfshark together with ExpressVPN and NordVPN served as the VPN providers that underwent testing across gaming activities and streaming activities and regular browsing operations. The handheld Wi-Fi network provided all the internet access through a laptop that used it for the network connection. One of the chosen VPN services enabled the laptop to create an encrypted VPN connection that transmitted all internet traffic through the secure tunnel. Testing network performance relied on using the evaluation tools Speedtest by Ookla, Fing and PingPlotter. Three performance assessment tools were used to measure important speed and latency and packet loss statistics under various conditions. The performance evaluation of the VPN service ran tests to show their effects on real-time network behavior. Figure 2 shows the evaluation testbed.

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

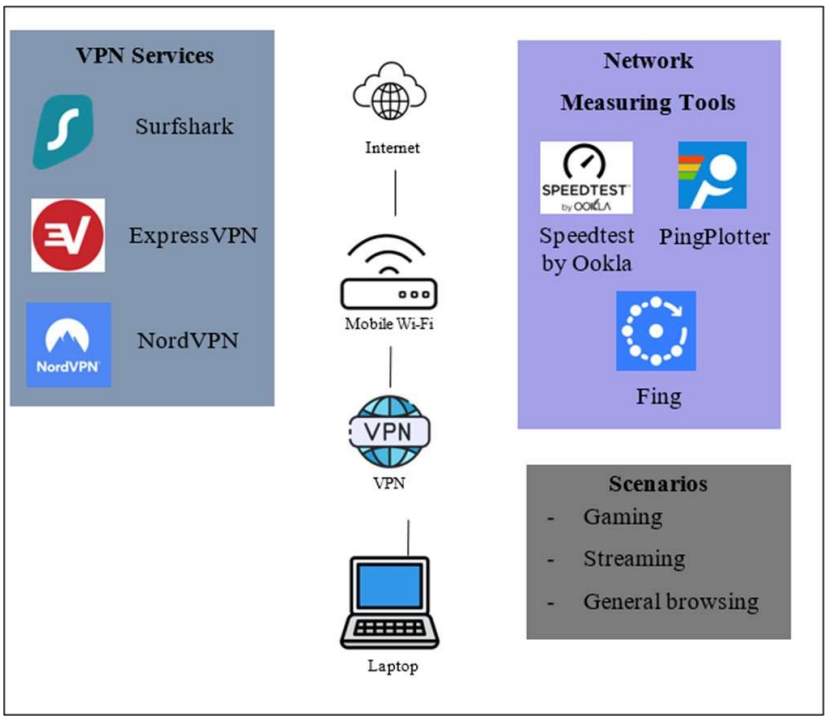

Figure 2: The Evaluation Testbed

RESULT AND DISCUSSION

This section presents the results derived from the testing procedures. The data gathered from the tests was averaged, and the key metrics which are upload and download speeds, latency, and packet loss were compared across the three VPNs in gaming, streaming, and general browsing scenarios.

Table 1: Average Overall Result

Scenario	VPN	Speedtest by Ookla		Pingplotter		Fing			
		Speed (Mbps)		Latency (ms)	Packet loss (%)	Speed (Mbps)		Latency (ms)	Packet loss (%)
		Upload	Download			Upload	Download		
Gaming	NordVPN	3.00	4.58	236.46	5.12	2.34	3.75	195.40	16.00
	ExpressVPN	3.72	4.52	209.84	3.32	2.23	3.21	259.60	15.33

	Surfshark	3.49	4.60	214.24	2.20	2.25	3.75	215.33	11.33
Streaming	NordVPN	3.49	4.34	263.94	3.86	2.31	3.11	228.53	8.00
	ExpressVPN	3.49	4.61	246.08	3.00	1.73	2.84	230.67	6.00
	Surfshark	3.10	4.82	247.94	4.30	2.58	3.62	222.00	5.33
General browsing	NordVPN	3.99	4.62	238.62	2.34	2.32	4.00	211.07	8.00
	ExpressVPN	3.55	4.51	230.62	1.56	3.05	4.01	218.00	5.33
	Surfshark	3.78	4.96	234.18	1.54	2.90	3.87	217.87	7.33

Table 1 shows the average result for the data that have been collected. For the gaming scenario, the upload speed monitored by Speedtest by Ookla was highest for ExpressVPN at 3.72 Mbps and lowest for NordVPN at 3.00 Mbps. The download speed, also monitored by Speedtest by Ookla, was highest for Surfshark at 4.60 Mbps and lowest for ExpressVPN at 4.52 Mbps. For latency measured using PingPlotter, the lowest latency was recorded by ExpressVPN at 209.84 ms, while the highest was recorded by NordVPN at 236.46 ms. Packet loss monitored by Pingplotter was lowest for Surfshark at 2.20% and highest for NordVPN at 5.12%. While using Fing, NordVPN has the best upload speed at 2.34 and ExpressVPN fall to the lowest at 2.23. For download speed both NordVPN and surfshark has recorded the same value which is 3.75 while ExpressVPN fall slightly behind at 3.21. NordVPN have recorded the lowest latency at 195.40 and the highest latency wa ExpreessVPN at 259.60. For packet loss, Surfshark got the best packet loss at 11.33 while NordVPN recorded a bit greater at 16.

Upload Speed

Speedtest by Ookla

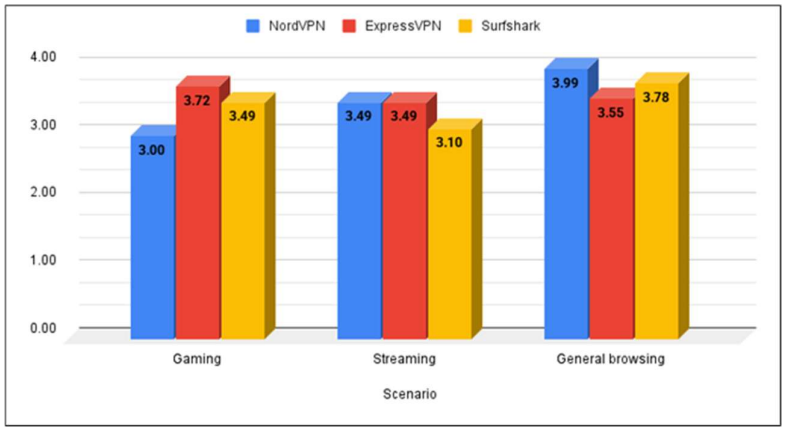

Figure 3: Upload speed by Speedtest by Ookla

Figure 3 highlighting the differences in upload speeds between the VPNs in this project indicate variation in server efficiency and traffic management. ExpressVPN's better upload speed indicates better server optimization and reduced congestion, and is thus better suited for data-heavy activities like file uploads. NordVPN's slower upload speed might be due to a higher server load or less ideal routing, which affects performance. Surfshark's consistent upload speed indicates a finely tuned server network that provides stable performance with no extreme fluctuations.

b) Fing

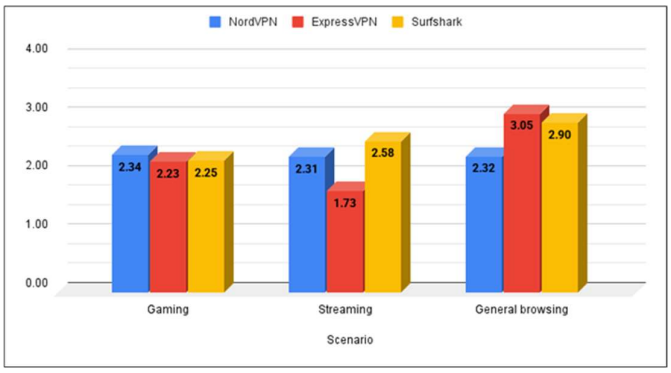

Figure 4: Upload speed by Fing

Figure 4 shows Fing's upload speed results alongside Speedtest by Ookla, representing differences in each tool's capacity to quantify network performance. NordVPN performed better in Fing's test, suggesting it may have better real-world performance during dynamic conditions. ExpressVPN slower upload speed in Fing's test could be due to momentary bottlenecks or geographical server differences. The tests show that VPN performance is influenced by different variables, including network traffic and server availability.

Download Speed

a) Speedtest by Ookla

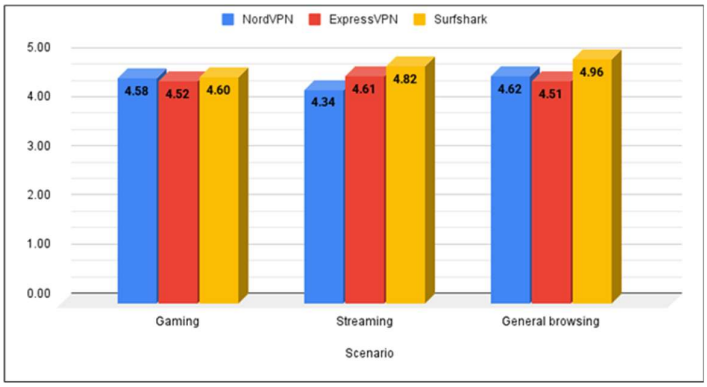

Figure 5: Download speed by Speedtest by Ookla

Figure 5 shows that download speed matters most for browsing and streaming. Surfshark's higher download speed shows that it performs better for big data transfers, making it an excellent choice for those who prioritize streaming or file downloading. ExpressVPN's comparatively slower download speed would imply that it prioritizes steady performance over speed. NordVPN's competitive but comparatively slower download speed suggests that server assignment and network traffic could influence performance.

b) Fing

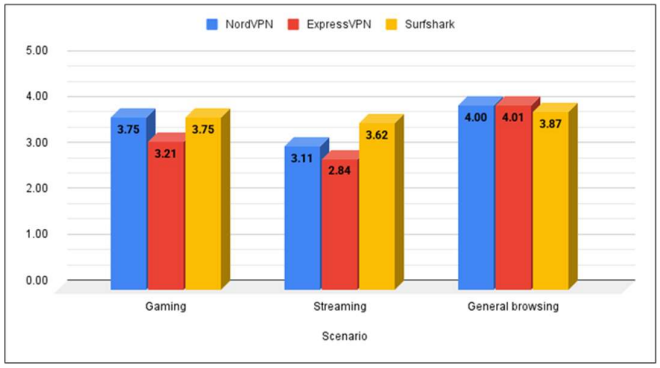

Figure 6: Download speed by Fing

Figure 6 presents that Speedtest by Ookla rankings varied slightly in Fing's test, reflecting that download speed varies with network conditions. NordVPN and Surfshark exhibited stable performance, indicating they provide stable speeds in practical use. ExpressVPN's lower speed could be influenced by the server load during testing. This variation reflects that VPN performance must be tested with multiple testing tools and under multiple conditions.

Latency

a) Pingplotter

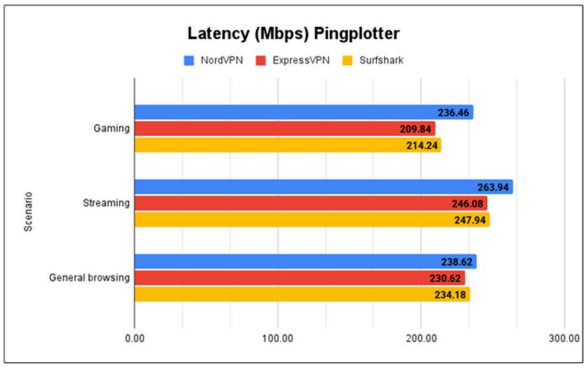

Figure 7: Latency by Pingplotter

Figure 7 discusses latency which is crucial for applications requiring real-time feedback such as gaming and streaming. Lower latency by ExpressVPN means that it uses more effective routing and server assignment, reducing delays. Higher latency by NordVPN may imply longer routes or more traffic on the network. Surfshark's decent latency performance suggests that it offers stable connections without significant delays.

b) Fing

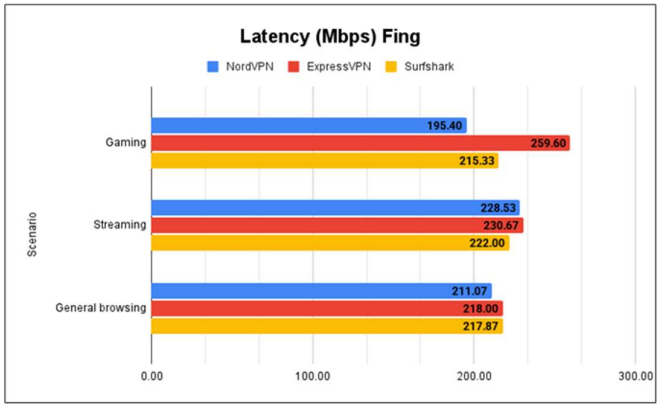

Figure 8: Latency by Fing

Figure 8 shows that Fing's latency outcomes varied from PingPlotter, demonstrating the influence of real-time network fluctuations on VPN performance. NordVPN's lower latency in this case means that it could be more effective at routing in certain situations. ExpressVPN's elevated latency in Fing's test could be the result of momentary server congestion. The results highlight the necessity of testing VPNs through multiple test mechanisms to gain an overall picture of performance.

Packet Loss

a) Pingplotter

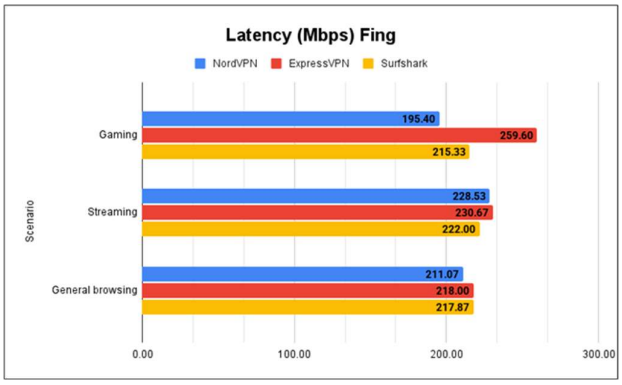

Figure 9: Packet Loss by Pingplotter

Figure 9 indicates packet loss impacts connection stability, an important factor for online gaming and streaming. The lower packet loss of Surfshark indicates it ensures robust server connectivity with less data loss. The higher packet loss of NordVPN may reflect network congestion or poor routing. The medium packet loss rate of ExpressVPN indicates that although it is performing well, there might be some disruptions occasionally due to dynamic network conditions.

b) Fing

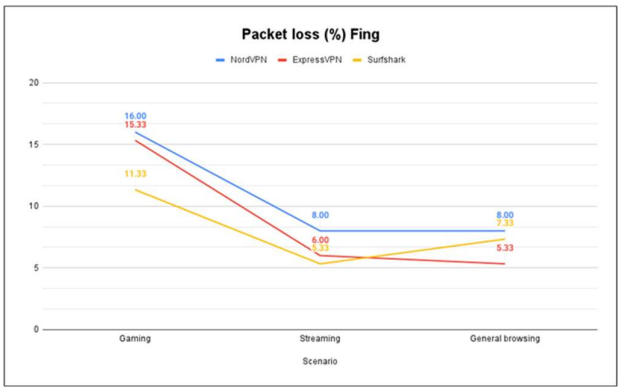

Figure 10: Packet Loss by Fing

Figure 10 illustrates Fing packet loss statistics, which were high, revealing how much the performance of the VPN was affected by network conditions. Surfshark recorded the lowest packet loss, thereby revealing its stability under varying conditions. High packet loss recorded with NordVPN reveals that it may suffer from occasional interruptions as a result of network congestion. ExpressVPN's mediocre performance indicates that although it tends to keep a stable connection, there might be a few instances of variability. These findings emphasize the importance of taking packet loss into account when choosing a VPN, particularly for users who need a stable connection..

Table 2: Average Different Server Location Result

Server Location	Speed (Mbps)		Latency)ms)	Packet loss (%)
	Upload	Download		
Asia	2.81	3.98	103.89	12.79
Australia	3.97	4.78	184.89	10.40
America	3.07	4.51	275.70	3.25
Europe	3.15	3.62	237.57	1.46
Africa	1.74	3.58	342.51	2.63

Table 2 shows the average result for different server location from the data that have been collected. While Africa had the lowest upload speed at 1.74 Mbps, Australia showed the best at 3.97 Mbps. Similar to this, Australia had the fastest download speed at 4.78 Mbps, whereas Europe and Africa both performed worse, falling below 4 Mbps. Asia had the lowest latency at 103.89 ms, whereas Africa had the greatest latency at 342.51 ms. While Europe had the lowest packet loss rate which only 1.46%, Asia had the highest rate at 12.79. These findings demonstrate how different server locations might affect network performance.

The findings collected from the testing on different server locations differ in VPN network performance based on upload speed, download speed, latency, and packet loss. A country from each continent was chosen to make this testing happen. The findings indicate that server location has a significant impact on network performance.

One of the main causes of differences in speed and latency is the physical distance between Malaysia and the VPN servers. Generally, the closer a server is to a user, the lower the latency and the higher the speed. This effect explains why the Asian server had the lowest latency since it is physically closer to Malaysia compared to other locations. The server in Africa had the highest latency due to its significant distance from Malaysia, which takes longer for data packets to travel between the user and the server. The farther the data needs to travel, the higher the opportunities for interruption and delay, and therefore more latency.

Network infrastructure is also a significant determinant of a VPN's performance. Australia recorded the best overall speed performance, owing to the well-developed internet infrastructure and high-capacity data centers therein. Africa recorded the worst upload speed, likely due to the fact that there are constraints in the network infrastructure in this continent. Fewer investments in high-speed networks, aging data transmission technologies, and reliance on lower-capacity undersea cables can negatively impact overall VPN performance. Europe and America's performance was mostly stable, which suggests that these two continents possess well-maintained and efficient network facilities to transport VPN traffic. Consistently low packet loss and stable speeds in Europe suggest robust network architecture with less congestion problems.

Packet loss is a vital metric when gauging the performance of a VPN since it affects the stability of an internet connection. The worst packet loss in the region was that of Asia, which is strange given that it's geographically near Malaysia. It could be the result of server congestion or inefficient routing protocols causing lost data packets. Severe packet loss can worsen user experience by leading to buffering in video streaming, lag in online games, and slower loading of web pages. Europe, however, registered the lowest rate of packet loss, reflecting a robust network with effective traffic management systems. It implies that VPN servers in Europe are better optimized, experiencing less congestion and superior traffic monitoring, which ensures stable data transmission. America and Africa packet loss rates point to medium network congestion or poor routing channels, possibly due to under-resourced servers or higher traffic volumes.

Finally, it is confirmed that the choice of VPN server location significantly affects network performance. Malaysian users wishing to get the best out of their VPN experience are advised to select server locations in Asia for the best latency, or Australia for the best speed. However, the high packet loss in Asia means that issues like server congestion or inefficiencies in routing need to be taken into account when selecting a server. In contrast, Europe's low packet loss and stable performance make it a good option for those who prefer reliability over raw speed. More importantly, the results highlight the importance of strategically selecting VPN servers based on the activity planned. For example, gaming users can take advantage of an Asian server, with its lower latency at the expense of increased packet loss. Meanwhile, those who value stable and ongoing browsing or streaming may like European servers for their low packet loss and acceptable performance balance.

Table 3: Multihop Server Result

VPN	Scenario	Speedtest by Ookla		Pingplotter				Fing			
		Speed (Mbps)		Latency (ms)		Packet loss (%)		Speed (ms)		Latency (ms)	Packet loss (%)
		Up	Down	S1	S2	S1	S2	Up	Down		
NordVPN	Gaming	0.53	2.00	306.30	328.90	1.08	9.43	0.20	3.33	303.33	16.67
	Streaming	0.53	2.38	298.60	316.00	1.53	7.52	0.20	3.30	308.67	26.67
	General browsing	0.47	1.53	293.60	312.50	1.12	8.79	0.23	3.03	309.33	10.00
Surfshark	Gaming	4.55	4.92	303.80	311.70	5.40	4.20	1.50	3.63	278.33	0.00
	Streaming	3.79	4.58	280.10	285.90	1.80	2.80	2.77	2.87	272.67	0.00
	General browsing	3.84	4.58	283.90	289.80	1.80	1.30	1.73	3.33	278.33	0.00

Table 3 shows the average result for different server location from the data that have been collected. For NordVPN, Speedtest by Ookla recorded the highest upload speed of 0.53 Mbps during the gaming and streaming scenario respectively and general browsing fell a little bit behind at 0.47 Mbps. As for download speed, Streaming recorded the highest at 2.38 Mbps and general browsing is the slowest at 1.53 Mbps. On the other hand, Fing recorded the highest upload speed of 0.23 Mbps during the general browsing scenario while the lowest upload speed of 0.20 Mbps during the gaming and streaming scenarios. While for the download speed, gaming recorded as the fastest at 3.33 ms and general browsing is the slowest at 3.03 ms. PingPlotter showed the highest latency of 328.90 ms at server 2 (S2) which is United States during the gaming scenario and the lowest latency of 306.30 ms at server 1 (S1) United Kingdom. For packet loss, S1 recorded the least packet loss at 1.08% during gaming while S2 recorded the most packet loss at 9.43% during gaming as well. On the other hand, Fing recorded the highest latency of 309.33 ms during the general browsing scenario and the lowest latency of 303.33 ms was recorded during the gaming scenario. The highest packet loss of 26.67% was recorded during the streaming scenario, while lowest packet loss of 10.00% during general browsing.

For Surfshark, Speedtest by Ookla recorded the highest upload speed of 4.55 Mbps during the gaming scenario, while the lowest upload speed of 3.79 Mbps occurred during the streaming

scenario. The highest download speed of 4.92 Mbps was recorded during the gaming scenario, and the lowest download speed of 4.58 Mbps was observed during both the streaming and general browsing scenarios. PingPlotter recorded the highest latency of 311.70 ms at Server 2 (UK) during the gaming scenario and the lowest latency of 280.10 ms at Server 1 (US) during the streaming scenario. The highest packet loss of 5.40% was recorded at Server 1 (US) during the gaming scenario, and the lowest packet loss of 1.30% was observed at Server 2 (UK) during the general browsing scenario. Fing recorded the highest upload speed of 2.77 Mbps during the streaming scenario and the lowest upload speed of 1.50 Mbps during the gaming scenario. The highest download speed of 3.63 Mbps was recorded during the gaming scenario, and the lowest download speed of 2.87 Mbps occurred during the streaming scenario. The highest latency of 278.33 ms was recorded during both the gaming and general browsing scenarios, while the lowest latency of 272.67 ms was observed during the streaming scenario. No packet loss was recorded in any scenario with Fing.

A multihop VPN is a feature that routes internet traffic through multiple servers instead of a single one. This approach enhances privacy by making it more difficult for third parties to track online activities, as the data is encrypted multiple times across different geographical locations. However, this added layer of security comes at the cost of increased latency and reduced internet speed due to the extended routing process. Among the VPNs tested in this project, NordVPN and Surfshark offer multihop functionality, whereas ExpressVPN does not provide this feature.

NordVPN demonstrated lower speed and higher latency compared to Surfshark. This may be due to the additional processing required for its encryption and routing strategies. The reduced performance in some scenarios suggests that NordVPN’s configuration may not be fully optimized for the Malaysian network environment, particularly for latency-sensitive applications such as gaming. Packet loss observed in certain scenarios further indicates potential inefficiencies in data transmission, possibly caused by congestion or extended routing paths. Surfshark exhibited better network performance, with higher speeds and lower latency across different scenarios. This suggests that Surfshark's server selection and network optimization provide more stable and efficient connections. The lower latency values indicate that Surfshark is better suited for tasks requiring real-time responsiveness, such as gaming

and streaming. Additionally, the lower packet loss rates suggest that Surfshark maintains a more consistent connection, which is beneficial for maintaining stable network performance during high-bandwidth activities.

The findings highlight the importance of selecting a VPN based on specific use requirements. NordVPN will not necessarily be the best option for those concerned with high performance and low latency. On the other hand, Surfshark appears to deliver a fairer performance, thus making it a preferable option for Malaysian users in quest for enhanced performance with multihop servers in a variety of scenarios.

CONCLUSION

To conclude, this study presents an in-depth comparative analysis of NordVPN, ExpressVPN, and Surfshark performance statistics in a mobile Wi-Fi network environment, with a specific focus on factors such as speed, latency, and packet loss during gaming, streaming, and general web browsing operations. The conclusion re-emphasizes the value in choosing a VPN that best addresses specific requirements and operations, and in the process, brings out the inescapable usability-performance trade-offs involved in using a VPN.

The outcomes of such a project not only inform users about making better choices but also stimulate VPN providers to correct performance weaknesses in their service offerings. In view of the inbuilt limitations in such a study, allowing for follow-up inquiry, such acquired knowledge forms a strong platform for future studies and development in VPN technology. By resolving the lack of scenario-specific performance measurement, such a study promotes a transparent and user-centric model for use of VPN, such that usability and performance requirements are both appropriately met. By supporting a transparent and user-centric approach in use of VPN, such an analysis promotes a model for usability and performance requirements to be effectively addressed.

REFERENCES

Abdulazeez, A. M., Salim, B. W., Zeebaree, D. Q., & Doghramachi, D. (2020). Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol. *International Journal of Interactive Mobile Technologies*, *14*(18). https://doi.org/10.3991/ijim.v14i18.16507

About Fing – Fing. (n.d.). Retrieved February 4, 2025, from https://help.fing.com/hc/en-us/articles/16670646589468-About-Fing#h_01J179XYZHJYW99TA6PRFK5WP3

Ahmad, M. (2022). Four important Wi-Fi design trends worth watching in 2022. *Electronic Products*, *64*(2), 14. https://www.edn.com/four-important-wi-fi-design-trends-worth-watching-in-2022/

AWS. (n.d.). *What is Network Latency?* Retrieved January 31, 2025, from https://aws.amazon.com/what-is/latency/

Benefits of Using Open Source VPNs in Enterprise Networks. (2024, June 18). https://www.netmaker.io/resources/open-source-vpn

Charan Sahu, T. (2022). Security and Privacy of Public WiFi. In *International Journal of Research Publication and Reviews* (Vol. 3, Issue 11).

Chua, C. H., & Ng, S. C. (2022). Open-Source VPN Software: Performance Comparison for Remote Access. *ACM International Conference Proceeding Series*, 29–34. https://doi.org/10.1145/3561877.3561882

Crawshaw, D. (2020). Everything VPN is New Again. *Queue*, *18*(5), 54–66. https://doi.org/10.1145/3434571.3439745

Dewi, S., & Sulistiyah, S. (2022). Analisa Virtual Private Network (VPN) IP Multi Protocol Label Switching (MPLS) Untuk Jaringan Wide Area Network (WAN). *Journal of Information System, Applied, Management, Accounting and Research*, *6*(1). https://doi.org/10.52362/jisamar.v6i1.662

Digital Samba. (2023, November). *Network Speed vs. Bandwidth vs. Throughput*. https://www.digitalsamba.com/blog/network-speed-vs-bandwidth-vs-throughput

Fayoumi, M. Al, Fawareh, M. Al, & Nashwan, S. (2022). Vpn and non-vpn network traffic classification using time-related features. *Computers, Materials and Continua*, *72*(2). https://doi.org/10.32604/cmc.2022.025103

Fortinet. (n.d.). *What Is Packet Loss?* Retrieved January 31, 2025, from https://www.fortinet.com/resources/cyberglossary/what-is-packet-loss

Frascolla, V., Cavalcanti, D., & Shah, R. (2023). Wi-Fi Evolution: The Path Towards Wi-Fi 7 and Its Impact on IIoT. *Journal of Mobile Multimedia*, *19*(1), 263–276. https://doi.org/10.13052/jmm1550-4646.19113

Fratel. (2020). *MEASURING MOBILE NETWORK PERFORMANCE: COVERAGE, QUALITY OF SERVICE AND MAPS*. www.fratel.org

Gao, D., Lin, H., Li, Z., Qian, F., Chen, Q. A., Qian, Z., Liu, W., Gong, L., & Liu, Y. (2021). A nationwide census on wifi security threats: Prevalence, riskiness, and the economics. *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*. https://doi.org/10.1145/3447993.3448620

Gentile, A. F., Macrì, D., De Rango, F., Tropea, M., & Greco, E. (2022). A VPN Performances Analysis of Constrained Hardware Open Source Infrastructure Deploy in IoT Environment. *Future Internet*, *14*(9). https://doi.org/10.3390/fi14090264

Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. *Victims and Offenders*, *16*(3). https://doi.org/10.1080/15564886.2020.1829224

Habibovic, S. (2019). *VIRTUAL PRIVATE NETWORKS*.

Haeruddin, H., Wijaya, G., & Khatimah, H. (2023). Sistem Keamanan Work From Anywhere Menggunakan VPN Generasi Lanjut. *JITU : Journal Informatic Technology And Communication*, *7*(2). https://doi.org/10.36596/jitu.v7i2.1086

Irsyad, I. D., & Mulyana, E. (2023). A Survey on Designs and Implementations of Virtual Private Network (VPN). *Proceedings of the International Conference on Electrical Engineering and Informatics*. https://doi.org/10.1109/ICEEI59426.2023.10346627

Karlina, S., Nugroho, B. S., Citra Atmaja, A. H., & Ismail, N. (2023). Ultra-Wideband Antenna for Bandwidth Enhancement Telkomsel Orbit Mobile Wifi. *Proceeding of 2023 9th International Conference on Wireless and Telematics, ICWT 2023*. https://doi.org/10.1109/ICWT58823.2023.10335417

Kumar Yedla, B. (2023). *Master of Science in Telecommunication Systems Performance evaluation of VPN solutions in multi-region kubernetes cluster*. www.bth.se

Li, Z., Dai, Y., Chen, G., & Liu, Y. (2023). Combating Nationwide WiFi Security Threats. In *Content Distribution for Mobile Internet: A Cloud-based Approach*. https://doi.org/10.1007/978-981-19-6982-9_8

Lugovic, S., Mrsic, L., & Korona, L. Z. (2019). Public WiFi Security Network Protocol Practices in Tourist Destination. *Communications in Computer and Information Science*, *1080 CCIS*. https://doi.org/10.1007/978-3-030-30143-9_27

NETSCOUT. (2020). *Visibility for Protecting VPN Availability and Assuring Performance*.

Ostroukh, A. V., Pronin, C. B., Podberezkin, A. A., Podberezkina, J. V., & Volkov, A. M. (2024). Enhancing Corporate Network Security and Performance: A Comprehensive Evaluation of WireGuard as a Next-Generation VPN Solution. *2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2024 - Conference Proceedings*. https://doi.org/10.1109/SYNCHROINFO61835.2024.10617501

PingPlotter. (n.d.). *How PingPlotter Works | Legacy*. Retrieved January 31, 2025, from https://www.pingplotter.com/legacy-manual/howitworks/

Ramezanpour, K., Jagannath, J., & Jagannath, A. (2023). Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective. In *Computer Networks* (Vol. 221). https://doi.org/10.1016/j.comnet.2022.109515

Reshef, E., & Cordeiro, C. (2022). Future Directions for Wi-Fi 8 and Beyond. *IEEE Communications Magazine*, *60*(10), 50–55. https://doi.org/10.1109/MCOM.003.2200037

Santoso, B., Sani, A., Husain, T., & Hendri, N. (2021). VPN SITE TO SITE IMPLEMENTATION USING PROTOCOL L2TP AND IPSEC. *TEKNOKOM*, *4*(1). https://doi.org/10.31943/teknokom.v4i1.59

Umaroh, L., & Rifauddin, M. (2020). IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) DI PERPUSTAKAAN UNIVERSITAS ISLAM MALANG. *BACA: JURNAL DOKUMENTASI DAN INFORMASI*, *41*(2). https://doi.org/10.14203/j.baca.v41i2.531

VPN Products Performance Benchmarks. (2023).

Zeyu, C. (2021). 6G, LIFI and WIFI Wireless Systems: Challenges, Development and Prospects. *2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2021*, 322–325. https://doi.org/10.1109/ICCWAMTIP53232.2021.9674090