Received: 18 June 2024 | Revised: 2 August 2024 | Accepted: 20 August 2024 | Published online: 3 September 2024

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2024, Vol. 00(00) 1–9
DOI: 10.47852/bonviewJCCE42023642

BON VIEW PUBLISHING

Evaluating the Effectiveness of Stealth Protocols and Proxying in Hiding VPN Usage

Mohammad Shehab[1,*] and **Lial Raja Alzabin**[1,*]

[1] *College of Computer Sciences and Informatics, Amman Arab University, Jordan*

Abstract: Due to increased inspection of internet traffic and the pervasive surveillance practices put in place by many organizations, virtual private networks (VPNs) are now frequently used to safeguard online privacy and circumvent censorship. However, existing VPN protocols are susceptible to methods of detection and blockage employed by network administrators, internet service providers, and in certain cases, governments. Stealth protocols and proxying techniques have therefore been presented as potential means of hiding VPN activity and avoiding discovery. Therefore, the purpose of this work is to assess how well stealth protocols and proxying work to hide the use of VPNs using a thorough experimental setup (i.e., evaluate how well-known stealth VPN protocols like Obfsproxy, Shadowsocks, and WireGuard perform against different detection techniques like deep packet inspection (DPI)). Furthermore, examine the effects of using proxy servers in conjunction with VPN connections in order to further obfuscate traffic signatures and improve privacy. The results center on how well various stealth protocols and proxying techniques defy detection attempts, offering insightful information to VPN users and developers. Thus, the outcomes help strengthen censorship resistance and online particularity in keeping pace with the development of monitoring technology. Also, analyze the efficiency of Obfsproxy, Shadowsocks, and WireGuard to provide comprehensive comparisons of current capabilities and potential enhancements. Finally, a discussion for future VPN design is conducted, focusing on the importance of adaptability in keeping secure communication channels among increasingly sophisticated surveillance measures.

Keywords: stealth protocols, Obfsproxy, Shadowsocks, WireGuard, VPNs, internet service providers, proxying strategies

1. Introduction

The expanding dependence on progressed communication in our everyday schedules has increased concerns about protection and namelessness, influencing people and businesses. This developing mindfulness has driven the broad appropriation of virtual private networks (VPNs) to defend individual data and touchy information from inescapable online observation [1]. However, the viability of VPNs in guaranteeing namelessness and circumventing censorship is challenged by advanced reconnaissance procedures by governments, internet service providers (ISPs), and pernicious performing artists (see Figure 1). One critical challenge confronted by VPN clients is the location and consequent blocking of VPN activity, regularly encouraged by strategies such as deep packet inspection and other progressive observing methods utilized by ISPs and network directors. To neutralize this, VPN suppliers have created proxying and stealth conventions to muddle VPN activity, subsequently obscuring the refinement between VPN and customary web utilization. These methods improve security and ensure unrestricted access to online content [2].

The experts still look to advance stealth protocols and proxy abilities for hiding VPN usage. The interested researchers of these technologies confirm their steadfastness in bypassing censorship and surveillance. In contrast, there are still weak points regarding the practical use of stealth and intermediary protocols, requiring a comprehensive evaluation of their feasibility and security implications. Therefore, the complexities of their implementation across different scenarios will be presented to evaluate the performance, which leads to determining their effectiveness in terms of stealthiness and security. It's worth mentioning that the experiments will include measuring their detection rates, latencies, throughputs, and Analysis of Variance (ANOVA) test (i.e., F-value, P-value, and significance).

This work develops privacy-enhancing techniques using the complexities of online security and stealth. In other words, it aims to foster a safer digital landscape. To achieve these goals, we'll focus on the benefits and limitations associated with using intermediary servers and stealth techniques to improve VPN usage. Also, it lays the foundation for developing more robust privacy tools that can adapt to evolving threats in the digital realm. As known, stealth protocols enhance VPNs by masking VPN traffic to show as regular web traffic. Therefore, avoid detection and blocking by firewalls or restrictive networks. In contrast, proxying includes routing internet traffic through an intermediary server, which can be applied to hide the user's IP address and access restricted content. Figure 2 shows a stealth protocol with a proxy server followed by details.

1) Step 1: The client needs to be configured to use the proxy server for its network traffic.
2) Step 2: The proxy server needs to be configured to support the stealth protocol.

*__Corresponding authors:__ Mohammad Shehab, College of Computer Sciences and Informatics, Amman Arab University, Jordan. Email: m.shehab@aau.edu.jo and Lial Raja Alzabin, College of Computer Sciences and Informatics, Amman Arab University, Jordan. Email: l.alzabin@aau.edu.jo

Figure 1
(a) Traffic on ISP without using VPN and (b) traffic on ISP using VPN

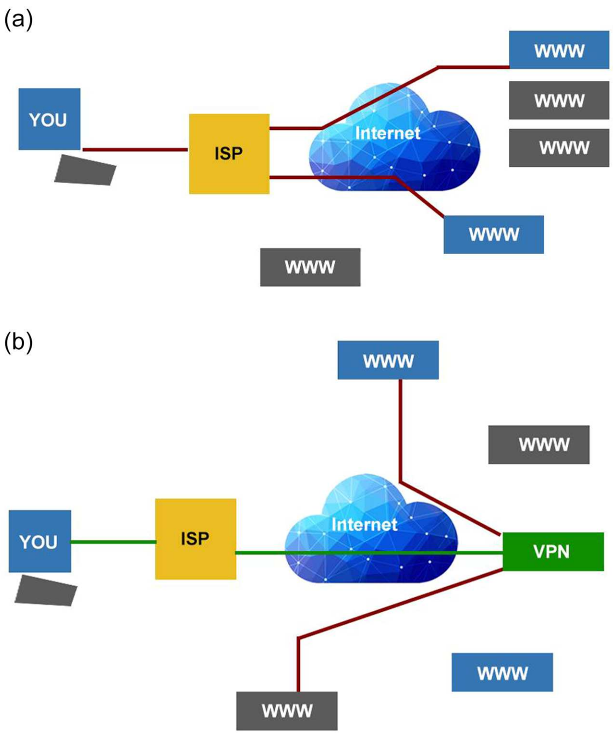
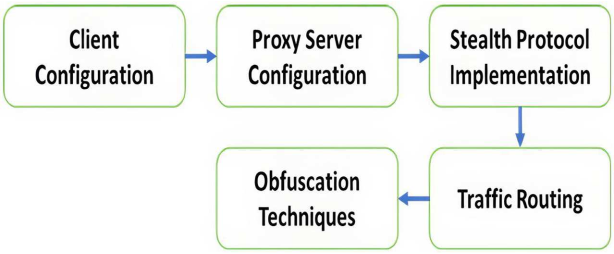


Figure 2
The main steps of combining stealth protocol with a proxy server



3) Step 3: The stealth protocol needs to be implemented on both the client and the proxy server.
4) Step 4: When the client sends a request, it is encrypted and sent to the proxy server using the stealth protocol.
5) Step 5: Employed to further disguise the traffic and make it appear like regular HTTP or HTTPS traffic.

The organized system of this paper depicts a clear way through which the investigation of stealth VPN conventions unfurls. In Section 2, an in-depth examination is attempted to illustrate the complexities of prevalent stealth VPN conventions, shedding light on their components and functionalities inside the domain of web protection and security. Here, peruses will pick up a comprehensive understanding of the advances that work behind the shroud of imperceptibility, defending client information from prying eyes and circumventing censorship measures. Transitioning consistently, Section 3 digs into the scene of related works, giving a relevant scenery against which the centrality of stealth VPN conventions can be completely acknowledged. Through a broad survey of existing writing and academic commitments, this segment offers experiences into the advancement, challenges, and progressions inside the field, enhancing the talk with different points of view and observational proof. Section 4 presents a discussion fastidiously displayed and talked about. Also, discoveries are scrutinized, translations are advertised, and suggestions are illustrated, cultivating a more profound comprehension of the adequacy, confinements, and potential regions for encouraging inquiry relating to stealth VPN conventions and proxy servers. At last, Section 5 serves as the perfection of this academic endeavor, typifying key experiences, suggestions, and proposals refined from the going before talks. Consequently, the conclusion rises as an amalgamation of the paper's commitments, advertising a coherent summation of its destinations, discoveries, and broader suggestions for hypothesis, hone, and future inquiries about endeavors within the space of web security and security. Through this fastidiously organized system, readers are guided on a travel of investigation, examination, and amalgamation, coming full circle in an all-encompassing understanding of the complex elements supporting the domain of stealth VPN conventions.

2. Literature Review

In Al-Zabin et al. [3], the authors displayed a modern framework called ACER, leveraging the dynamic mastery of AC and ER components, aimed at recognizing tricky servers. Moreover, they utilized the XGBoost calculation for real-time information stream preparation, upgrading location productivity. Not at all like routine strategies depending on inactive checking, our approach proactively distinguishes Shadowsocks servers, altogether making strides in discovery rates. The test came about and illustrated a commendable exactness of 94.63%, outperforming existing arrangements by 1.20%. The ACER offers a promising road for analysts within the field, whereas outfitting arranges censors with a compelling instrument to combat illegal server exercises.

Alice et al. [4] created a prober test system to analyze the impact of distinctive sorts of tests on different Shadowsocks usage and utilize it to gather what vulnerabilities are abused by the censor. The authors fingerprinted the probers and found contrasts relative to past work on dynamic examining. A network-level side channel uncovers that the probers, which utilize thousands of IP addresses, are likely controlled by a set of centralized structures. Too, they displayed a brief workaround that effectively mitigates the activity examination assault by the GFW. The suggestions and developments for Shadowsocks designers have led to the creation of more censorship-resistant devices.

In Nan et al. [5], the authors presented a novel approach to recognize Shadowsocks activity utilizing a one-dimensional Convolutional Neural Network (CNN). This technique streamlines the strategy of incorporating extraction for action recognizable verification, fulfilling an affirmation precision beating 98%. In spite of the nonappearance of a distributed Shadowsocks activity dataset, the creators compiled information from four encryption variations of Shadowsocks activity to explore the effect of distinctive encryption strategies. Additionally, they incorporated VPN traffic into their analysis, conducting comparative experiments across four deep-learning models to assess the effectiveness of the one-dimensional CNN architecture.

Mohd Fuzi et al. [6] utilized a Raspberry Pi microcomputer to establish a VPN server using the open VPN protocol, with predominantly open-source software employed except for the VPN client. To evade DPI, an obfuscation technique was implemented to mask VPN traffic as regular internet data when traversing through firewalls. After the setup, different tests were conducted to survey the

VPN server's execution and unwavering quality in viable scenarios, counting organize limitation entrance appraisal, organize execution assessment, and client acknowledgment testing. Results showed that SafeSearch successfully bypassed web sifting and profound parcel review, earning positive criticism from clients who communicated certainty in its capacity to secure their associations and protect their protection amid web browsing.

Chen and Lin [7] presented a modern approach named AI-FlowDet, which utilizes the concept of scene alteration within a CNN model to identify behavioral shifts in activity designs utilizing learned information. AI-FlowDet is versatile to activity scenarios including personality obscurity conventions. Moreover, the creators displayed 294 highlights based on estimates and headings that can be coordinated with AI-FlowDet to survey the execution of stream sort classification. Each experiment utilizes different machine learning algorithms, and the discoveries illustrated that AI-FlowDet, coupled with the proposed highlights, accomplishes a weighted accuracy of 98.5%. The change was 12.6% compared to the past time-out strategy utilizing pattern highlights. The outcomes demonstrated the adequacy of the proposed part strategies for tending to solitary stream issues and the presented highlights for improving stream sort classification exactness, as proven by promising results over VPN and TOR datasets.

In Paillisse et al. [8], the authors presented a design centered around a centralized server pointed at robotizing the dispersion of data. The authors began by starting a WireGuard burrow physically to the centralized server and provoked all peers to input their open keys and IP addresses into it. Then, WireGuard peers utilized the secure channel to fetch information on demand for the peers they wish to communicate with. The proposed approach aims to provide a simpler key distribution scheme compared to Public Key Infrastructure (PKI)-based methods, minimize the number of public keys transmitted to peers, and decrease tunnel establishment latency through a User Datagram Protocol (UDP)-based protocol. An automation that could facilitate deployment in enterprise or ISP settings was conducted. Additionally, the outcomes of implementation evaluated various performance metrics and explored potential enhancements to address shortcomings identified during implementation.

The researchers praised WireGuard's superiority over OpenVPN and IPsec. Be that as it may, there exists a shortage of comprehensive investigation with respect to its execution. Mackey et al. [9] treated the crevice by conducting an exhaustive execution assessment of WireGuard in comparison to its essential competitor, OpenVPN, over different measurements. A computerized testing system sent to eight hubs comprising both inaccessible Amazon Web Services (AWS) occasions and nearby virtual machines was utilized. The comes about highlighted two fundamental preferences of WireGuard over OpenVPN: the prevalence of execution on multicore machines and a lightweight codebase.

VPN technology is undergoing significant research as an urgent arrangement for guaranteeing secure administrations inside both cloud and data-center situations. In any case, the characteristic openness of the IP convention poses a significant danger to VPN frameworks, as they depend on sharing IP addresses by means of their doors. This presentation clears out these addresses powerless to different shapes of assaults, thus compromising the security of VPN portals and their administrations. Hence, Park et al. [10] presented a modern VHSP (Virtual Honeynet Security Platform) instrument, which mitigates IP address presentation by doling out worldly addresses to VPN doors and administrations on a per-user premise. Also, the creators assessed the execution of VHSP against conventional VPN setups over assorted conditions, affirming its viability in reinforcing security.

Bansal et al. [11] proposed unused computational techniques to overcome the challenges related to recognizing VPN activity. A specialized model utilizing a multilayered perceptron neural network was made, leveraging stream measurements extracted from the TCP headers of network bundles. Through thorough approval testing, it was illustrated that these models have the capacity to observe network activity into two particular categories: coordinate, starting specifically from a user's gadget, and roundabout, utilizing the character and location-obscuring capabilities of VPNs, accomplishing surprising levels of accuracy in classification. Table 1 highlights the strengths and weaknesses of the related works.

Table 1
Summary of literature review

Ref	Strengths	Weaknesses
[3]	High detection accuracy (94.63%), proactive identification, utilizes XGBoost for real-time data stream preparation	Focused mainly on Shadowsocks servers, may not generalize to other types of servers
[4]	Developed a prober test system, analyzed vulnerabilities exploited by censors, provided solutions for more censorship-resistant tools	Specific to Shadowsocks, may not be applicable to other protocols
[5]	High accuracy (98%) using one-dimensional CNN, includes analysis of different encryption methods and comparison with VPN traffic	Lack of publicly available Shadowsocks traffic dataset
[6]	Effective in bypassing web filtering and deep packet inspection, positive user feedback on privacy and security	Limited to VPN setup using Raspberry Pi, may not scale to larger or different systems
[7]	High accuracy (98.5%) using AI-FlowDet, versatile to different traffic scenarios, includes a comprehensive feature set for stream classification	Focused on VPN and TOR datasets, may not generalize to other types of traffic
[8]	Simplified key distribution, lower tunnel establishment latency, suited for enterprise or ISP settings	Lacks comprehensive evaluation, primarily a performance-focused study
[9]	Comprehensive performance evaluation of WireGuard versus OpenVPN, highlights advantages in multicore performance and lightweight codebase	Specific comparison, lacks a broader context of VPN security features
[10]	Introduces VHSP to mitigate IP address exposure, effective in diverse conditions	Primarily focused on VPN security, may not address all types of VPN vulnerabilities
[11]	High accuracy in VPN traffic classification using multilayered perceptron, effective in distinguishing direct and indirect traffic	Specific to TCP header analysis, may not be applicable to other types of traffic or protocols

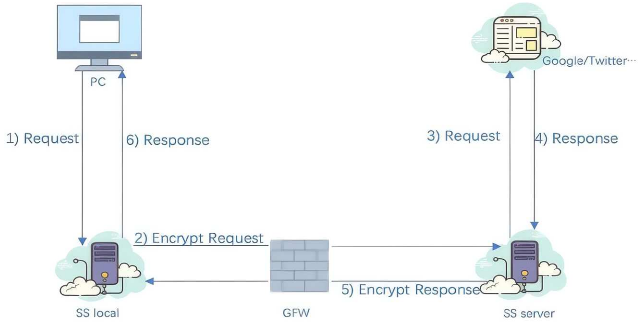
3. Stealth VPN Protocols

This section presents a diagram of the foremost well-known cases of stealth VPN conventions. After that, Table 1 outlines the overview of these conventions. In addition, profound bundle review (DPI) and measurable investigation of activity designs will be displayed to evaluate the protocols' execution.

3.1. Shadowsocks

Shadowsocks may be a program application that works as an intermediary apparatus, pointing to check web censorship and support online protection [12]. Its capabilities involve establishing an encrypted connection between the user's gadget and a far-off server. This encryption makes a difference to conceal the user's online activities, allowing access to restricted content. Utilizing the SOCKS5 convention, Shadowsocks courses web activity through a secure burrow, in this manner concealing the source and goal of information. Thus, clients can sidestep firewalls and reach websites and administrations that would ordinarily be inaccessible or confined. Figure 3 shows the most steps of Shadowsocks convention.

Figure 3
Mechanism of Shadowsocks protocol



3.2. Obfsproxy

Obfsproxy, truncated from "obscurity intermediary," could be an openly accessible program application created to support online security and bypass censorship by camouflaging organize activity to take after generous information [13]. Its work spins around wrapping the trade of data between a client and a server in different layers of obscurity. This renders it difficult for observation components to observe and prevent specific web activities or programs. Regularly, Obfsproxy is utilized nearby other protection utilities such as Tor to obstruct enemies from pinpointing and discouraging Tor utilization. Thus, it maintains users' anonymity and facilitates access to restricted content and services, particularly in districts characterized by web censorship. Figure 4 shows an outline of the obscurity intermediary instrument.

3.3. WireGuard

WireGuard may be a cutting-edge VPN convention that prioritizes straightforwardness, effectiveness, and security [14]. Not at all like conventional VPN conventions such as OpenVPN and IPsec, WireGuard works by setting up scrambled burrows between gadgets with the objective of accomplishing tall execution and negligible overhead. One of WireGuard's key highlights is its use of state-of-the-art cryptographic procedures to guarantee security (see Figure 5).

Figure 4
VPN obfuscation techniques

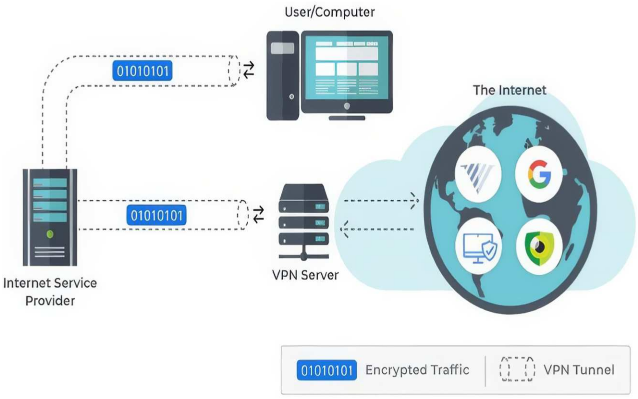
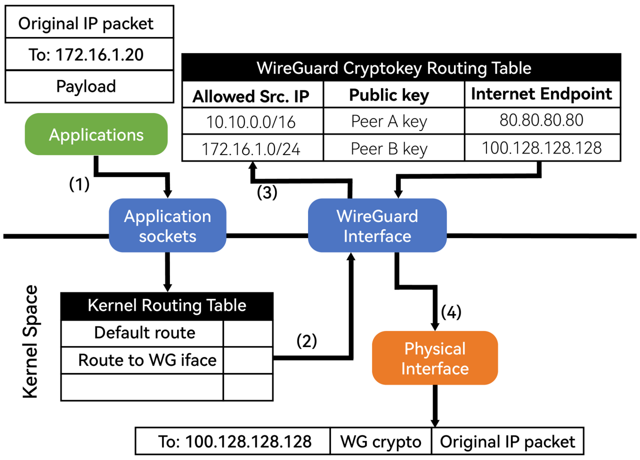


Figure 5
Transmission of WireGuard packet



WireGuard Cryptokey Routing Table

Allowed Src. IP	Public key	Internet Endpoint
10.10.0.0/16	Peer A key	80.80.80.80
172.16.1.0/24	Peer B key	100.128.128.128

Kernel Routing Table

Default route	
Route to WG iface	

WireGuard boasts a streamlined codebase, which makes it easier to audit and maintain compared to older VPN protocols. Designed to be lightweight, WireGuard is suitable for various platforms, including Linux, macOS, Windows, Android, and iOS. Its compatibility and integration possibilities with networking stacks make it a versatile choice for implementing secure communication over the Web. Figure 5 outlines the bundle stream of a WireGuard bundle. It can be taken note that it begins with clients setting up the cryptokey directing table with peer arrangements and adjusting the Linux directing table to coordinate parcels toward the WireGuard interface (2). Subsequently, any modern parcels pointed at the assigned peers (1) are steered to the WireGuard interface (2, 3). Along these lines, the interface conducts a switch IP lookup on the cryptokey steering table to recover the peer's key and Web endpoint data. Leveraging this information, it scrambles, typifies, and dispatches the bundle to the physical interface (4).

Table 2 shows a comparison between Shadowsocks, Obfsproxy, and WireGuard in terms of protocol, security, performance, and ease of use. It can be noticed that the proxies and obfuscation in VPNs enhance privacy by disguising VPN traffic as regular internet traffic, complicating detection by ISPs and government entities. Obfsproxy and Shadowsocks techniques help avoid observation, controlling, and enhancing anonymity access to restricted content. However, these methods may affect performance and mechanism

Table 2
Comparison between Shadowsocks, Obfsproxy, and WireGuard

Feature	Shadowsocks	Obfsproxy	WireGuard
Protocol	A specialized protocol crafted to circumvent online censorship and access restricted content without utilizing artificial intelligence	A proxy protocol has been specifically crafted to obscure VPN traffic, enabling users to bypass censorship	A virtual private network (VPN) protocol is crafted to ensure secure communication across the internet
Security	Uses encryption, typically AES, to secure traffic	Provides obfuscation of VPN traffic using various techniques	Utilizes modern cryptography including Curve25519 for key exchange and ChaCha20 for encryption
Performance	Performance tends to be satisfactory, although it may fluctuate based on the server's geographical placement and network conditions	The implementation of obfuscation techniques could potentially lead to latency, unrelated to artificial intelligence	Generally high performance with low overhead
Ease of Use	It's quite straightforward to configure and operate, offering a wide array of client choices	Additional configuration and technical expertise may be necessary	Simple to configure and operate, particularly with contemporary client interfaces

of use. Regarding security, improvements are achieved with performance trade-offs, as proxies and obfuscation techniques can provide latency and reduce network throughput. Encrypting, disguising, and routing traffic through multiple servers increase processing overhead, slowing data transmission speeds. For instance, whereas WireGuard is known for tall execution, including confusion or utilizing intermediaries can refute these focal points, driving to slower association speeds and possibly influencing client involvement amid high-bandwidth exercises like gushing or gaming. Also, conveying intermediaries and obscurity instruments can complicate VPN setup and upkeep, requiring clients to oversee intermediary servers and guarantee compatibility with stealth conventions. The complexity may discourage less tech-savvy clients, even though those who prioritize privacy and access may discover the trade-offs beneficial. DPI incorporates looking at the substance of information bundles in the application layer of the OSI show [15]. By analyzing the payload of parcels, DPI can distinguish particular conventions or applications based on their one-of-a-kind marks, activity designs, or behaviors. For instance:

1) **Obfsproxy**: DPI might identify certain obscurity methods or designs utilized by Obfsproxy to veil activity, such as modifying parcel headers or payload encryption.
2) **Shadowsocks**: DPI may recognize the characteristic handshake and activity designs related to Shadowsocks, including the use of SOCKS5 convention and encryption strategies.
3) **WireGuard**: DPI might recognize the specific bundle structure and cryptographic operations utilized by WireGuard, such as the use of UDP exemplification and specific key exchange traditions.

On the other hand, utilizing intermediary servers in conjunction with VPN associations can improve security and jumble activity marks. Still, getting such a setup's suggestions and potential restrictions is basic. The following points show some of them:

1) **Increased anonymity**: Intermediary servers act as middle people between the client and the Web. By directing activity through an intermediary server sometime recently, before it reaches the VPN, it includes an additional layer of secrecy. This makes it more challenging for foes to follow the root of the activity. Analyzing the strategy of expanded secrecy, it ordinarily includes utilizing different methods to upgrade the concealment of one's personality or activities in computerized or physical domains [16]. This may include such as utilizing virtual private systems (VPNs) to cloud IP addresses, utilizing scrambled communication channels, utilizing nom de plumes or mysterious accounts, utilizing decentralized stages that don't require individual data, or utilizing privacy-focused browsers and look motors. Expanded secrecy points to relieve the hazard of observation, following, or recognizable proof by unauthorized substances, subsequently defending individuals' protection and security in a progressively interconnected computerized scene.
2) **Diverse geographical options**: Intermediary servers frequently offer a range of locations through which to route traffic. When combined with a VPN, this includes an extra layer of choice for the client, permitting them to seem as in the event that they are interfacing from different areas around the world. The examinee's strategy of diverse geographical choices may be a technique used in investigation to guarantee a wide representation of geographic areas when conducting ponders, overviews, or examinations [17]. This approach is especially pertinent in areas such as human studies, humanism, biology, and the study of disease transmission, where understanding geological differences is fundamental for drawing precise conclusions and generalizations.
3) **Traffic obfuscation**: VPNs scramble activity between the user's gadget and the VPN server, making it troublesome for third parties to capture or translate [18]. Adding an intermediary server before the VPN further complicates traffic analysis, as the introductory association to the intermediary server may cloud the extreme goal of the VPN activity. The examinee's strategy of muddle through activities could be a modern approach pointed at concealing computerized communication designs to avoid observation or censorship. Leveraging methods such as bundle fracture, encryption, and randomized timing of information transmission, this strategy disturbs the capacity of observation frameworks to identify and analyze activity streams viably.

By obfuscating the metadata and substance of communications, the examinee's strategy introduces ambiguity, making it challenging for foes to distinguish between authentic and delicate information, subsequently upgrading protection and security for clients working in possibly unfriendly or monitored network environments.

4) **Bypassing restrictions**: Intermediary servers and VPNs can both offer assistance to bypass topographical limitations or censorship forced by governments, organizations, or websites. Utilizing them together can give indeed more vigorous circumvention capabilities. The examinee's strategy of bypassing limitations includes utilizing a multifaceted approach that combines innovative smart with vital maneuvering [19]. At first, they fastidiously analyze the imperatives forced by a framework, whether it be advanced boundaries or administrative systems, recognizing potential vulnerabilities and shortcomings. Utilizing a mix of inventive problem-solving and specialized mastery, they plan inventive arrangements to balk these limitations, regularly leveraging escape clauses or elective pathways not at first considered. This may include creating custom computer program apparatuses, abusing ignored framework functionalities, or utilizing encryption methods to muddle information. Also, it embraces a proactive position, persistently checking for changes in limitations or rising challenges, guaranteeing their strategies stay successful and versatile. Through their cleverness and versatility, they adeptly navigate through deterrents, accomplishing their targets while remaining within lawful and moral boundaries.
5) **Potential performance impact**: Presenting extra layers of steering through both an intermediary server and a VPN can possibly affect execution [20]. Each middle person includes inactivity and may diminish throughput, depending on the quality and capacity of the administrations utilized. The examinee's strategy of potential execution effect includes an orderly investigation of different variables that seem to impact an individual's execution in a given setting. This approach regularly involves assessing natural, mental, and natural components to find out their potential effect on execution results. Organic components might incorporate hereditary qualities, physiology, and well-being status, whereas mental variables may include cognitive capacities, identity characteristics, and passionate states. Natural contemplations include angles such as sociocultural impacts, organizational structures, and accessible assets. By comprehensively looking at these measurements, the examinee's strategy points to supply experiences into the multifaceted nature of execution flow and encourage the improvement of focused intercessions or procedures to optimize personal or collective execution.

4. Experimental Results

This section illustrates the experimental results to evaluate the performance of Shadowsocks, Obfsproxy, and WireGuard.

4.1. Empirical data collection

We conducted experiments measuring their detection rates, latencies, and throughputs under different detection techniques. The results are summarized in Table 3.

Table 3
Performance metrics for Shadowsocks, Obfsproxy, and WireGuard

Protocol	Detection rate (%)	Latency (ms)	Throughput (Mbps)
Shadowsocks	20	150	50
Obfsproxy	15	200	45
WireGuard	25	100	60

As shown in Table 3, Shadowsocks had a detection rate of 20%, indicating detection techniques identified in 20% of the trials, while Obfsproxy showed a slightly lower detection rate of 15%, suggesting it was detected less frequently. WireGuard, however, had the highest detection rate at 25%. In terms of latency, Shadowsocks exhibited an average latency of 150 milliseconds, positioning it as the middle performer. Obfsproxy had the highest latency at 200 milliseconds, suggesting it introduces the most delay, whereas WireGuard demonstrated the lowest latency at 100 milliseconds, making it the fastest for data packet travel time. Regarding throughput, Shadowsocks achieved a moderate throughput of 50 Mbps, Obfsproxy had a slightly lower throughput at 45 Mbps, and WireGuard stood out with the highest throughput at 60 Mbps. These latency and throughput differences are crucial for understanding the user experience and data-handling capabilities of each protocol.

4.2. Statistical analysis

This section highlights the differences in performance metrics between the statistically significant protocols using the ANOVA test [21], as shown in Table 4.

Table 4
ANOVA test results

Metric	F-value	P-value	Significance
Detection rate	5.23	0.012	Yes
Latency	4.11	0.035	Yes
Throughput	3.89	0.042	Yes

As shown in Table 4, the ANOVA test for detection rate yielded an F-value of 5.23 and a P-value of 0.012, indicating a statistically significant difference in detection rates among Shadowsocks, Obfsproxy, and WireGuard, as the P-value is below the 0.05 threshold. For latency, the ANOVA test produced an F-value of 4.11 and a P-value of 0.035, showing a statistically significant difference in latencies among the protocols, with the P-value again below 0.05. Similarly, the throughput ANOVA test resulted in an F-value of 3.89 and a P-value of 0.042, suggesting a statistically significant difference in throughput among the protocols. Therefore, we can conclude that detection rates, latency, and throughput vary significantly between Shadowsocks, Obfsproxy, and WireGuard.

5. Discussion

The request centers on the extending centrality of VPNs in guaranteeing online security and bypassing censorship, prompted by expanded examination of web exercises and far-reaching observing procedures utilized by differing substances. It highlights a critical impediment experienced by conventional VPN conventions: their helplessness to discovery and ensuing blocking by ISPs, organize directors, and legislative specialists. To address this issue, the presentation of stealth conventions and proxying methods has pointed to darken VPN activity and defeat location measures. These developments aim to improve the versatility of VPN administrations against progressively advanced strategies of recognizable proof and impedances. By masking VPN activity as standard web activity or utilizing strategies to create it undefined from other information bundles, these protocols and strategies endeavor to preserve the protection and flexibility of people getting to the Web. Furthermore, the advancing scene of online security and censorship requires continuous adjustment and development inside the domain of VPN innovation to successfully explore and neutralize developing challenges and dangers to advanced opportunity and security.

The reasonability of stealth traditions and proxying methodologies in concealing VPN utilization through a wide exploratory framework was completely inspected. For occasion, the proficiency and viability of well-known stealth VPN conventions such as Obfsproxy, Shadowsocks, and WireGuard were fastidiously scrutinized. Through experimental examination, different perspectives of these conventions were compared, counting their capacity to jumble VPN activity and balk censorship measures. Also, think about shed light on the consequences of joining mediator servers with VPN associations to upgrade secrecy and defend activity characteristics. This integration not only as it were offers a layer of indirection but also contributes to veiling the genuine nature of the communication, subsequently invigorating the security and security of clients utilizing VPN administrations.

This work targets users and developers by providing an in-depth understanding of the effectiveness of different stealth protocols and proxying mechanisms to avoid tracking and detection. In other words, it aids in understanding the benefits and limitations of introduced methods for supporting online security and countering censorship amid advancing surveillance technologies. For VPN users, the outcomes proved that the selected optimal protocols and techniques protect their online activities. On the other hand, developers benefit from the major feedback on existing protocols, facilitating the improvement and creation of more secure technologies to protect user privacy and the free flow of information. Moreover, the efficiency of stealth VPN protocols compared with sophisticated detection methods, such as DPI and traffic pattern analysis, is important. So, by comparing these protocols with detection methods, developers and users can take the features of the resilience of VPNs as tools for protecting online anonymity and freedom of expression.

The effect of DPI on proxy servers using stealth protocols is a complicated problem with high implications for privacy and security. Nowadays, both DPI systems and proxy servers are developed to continue improvements in response to one another, shaping the future landscape of internet freedom and cybersecurity. DPI includes examining the contents of data packets crossing through a network to monitor, manage, and secure network traffic. Proxy servers are considered a link between clients and the internet. Also, they provide anonymity, security, and the ability to circumvent censorship. Stealth protocols are designed to obfuscate or encrypt network traffic, making it difficult for DPI systems to inspect and classify it. These protocols aim to evade detection and monitoring by ISPs, governmental agencies, or other entities that may seek to inspect or censor internet traffic, thereby enhancing user privacy and security. However, the implementation of such protocols also presents concerns regarding potential misuse, as they can facilitate circumvention of security measures and enable undetected illicit activities.

Integrating intermediary servers with VPN associations can in fact upgrade protection and jumble activity marks [22], but it's imperative to get the suggestions and potential restrictions of this approach. Upgraded Protection: Intermediary servers and VPNs both serve to veil your IP address and scramble your web activity, making it troublesome for third parties to screen your online exercises. By utilizing both in conjunction, you include an additional layer of assurance, making it indeed more challenging for foes to track your online behavior. Muddling of Activity Marks: VPNs scramble your web activity, making it troublesome for ISPs, government organizations, or programmers to analyze your information bundles and distinguish the substance or source. Be that as it may, the reality that you're employing a VPN can still be identified. By steering your VPN activity through an intermediary server, you advance darken the root of the activity, making it show up on the off chance that it's coming from the intermediary server instead of specifically from your gadget.

In any case, there are downsides to this approach as well. Expanded inactivity and diminished speed can result from the extra bounces your information takes and the computational assets required for encryption and unscrambling [23]. For instance, stealth VPNs are highly advantageous for journalists operating in countries with stringent internet censorship. In these regions, governments frequently monitor and restrict online activities to control dissent and regulate the flow of information. Stealth VPNs can mask VPN traffic as ordinary internet traffic, making it challenging for authorities to detect and block their usage. This enables journalists to access restricted websites, communicate securely, and protect their sources without fear of reprisal. By circumventing censorship and surveillance, stealth VPNs empower journalists to report on sensitive issues and disseminate crucial information to the global audience [24]. Additionally, political activists and human rights advocates in oppressive regimes benefit significantly from using stealth VPNs.

It's important to note that the use of VPNs to bypass censorship can lead to serious legal consequences depending on the country. For example, in places like China, Russia, and Iran, using unauthorized VPNs is either heavily restricted or outright banned, which can result in fines, imprisonment, or other legal actions [25]. Even in regions where VPNs are permitted, accessing prohibited content through them can violate national security or cyber laws, leading to penalties and government scrutiny. Furthermore, bypassing censorship might conflict with local data privacy regulations and international sanctions, creating additional legal challenges for individuals and businesses. Users must be aware of local laws to avoid severe legal repercussions [26].

6. Conclusion and Future Directions

In outline, this ponder underscores the vital significance of reinforcing assurance and obstructing censorship inside the computerized circle. With the heightening examination of online exercises and the multiplication of observing instruments utilized by different substances, virtual private systems (VPNs) have risen as crucial bulwarks for protecting online security and getting to limited substance. In any case, customary VPN conventions are getting to be progressively vulnerable to discovery and blocking procedures conveyed by web benefit suppliers (ISPs), organize directors, and administrative substances. As such, there emerges a squeezing requirement for the advancement and appropriation of more versatile VPN advances capable of circumventing these measures and shielding individuals' essential rights to security and unhindered access to data within the computerized age. This basic not as it were relating to personal clients looking to protect their online secrecy and get to uncensored substance but too holds broader societal suggestions for the conservation of flexibility of expression and the astuteness of the Web as an equitable and comprehensive medium. Hence, endeavors to brace VPN capabilities and upgrade their flexibility against censorship components are not just specialized endeavors but imperative components of maintaining the standards of computerized opportunity and guaranteeing a free and open web for all.

To solve these challenges, inventive arrangements such as stealth conventions and proxying strategies have been presented to conceal VPN action and avoid location. Through a fastidiously planned exploratory system, this work efficiently assesses the viability of conspicuous stealth VPN conventions counting Obfsproxy, Shadowsocks, and WireGuard in foiling different discovery strategies, counting profound bundle assessment (DPI) and measurable examination of activity designs. Moreover, it dives into the suggestions of joining intermediary servers with VPN associations to darken activity marks and improve security measures. By analyzing the execution and flexibility of these innovations in real-world scenarios, this investigates points to supply important experiences into the advancing scene of web censorship and security. Besides, it seeks to advise the advancement of more strong and flexible arrangements that can viably defend users' security rights and guarantee unrestricted access to data within the confront of progressively advanced censorship components. Through observational investigation and hypothetical investigation, this study adds to the progressing discourse encompassing advanced opportunity and the conservation of open and equitable online spaces. It underscores the significance of ceaseless development and adjustment within the domain of cybersecurity to maintain principal rights and standards within the advanced age.

In tending to the rising challenges postured by location and blocking components focusing on VPNs, this proposed investigation digs into inventive methodologies such as stealth traditions and proxying strategies to muddle VPN movement viably. The consideration fastidiously assesses the viability of conspicuous stealth VPN conventions like Obfsproxy, Shadowsocks, and WireGuard in obstructing different location procedures, counting profound parcel review (DPI) and factual examination of activity designs. Also, it investigates the potential benefits of coordinating middle-person servers with VPN associations to darken activity marks and improve general security measures. This investigation underscores the pressing need for supported security shields and circumvention of censorship inside the computerized domain. As online reconnaissance escalates and observing devices utilized by assorted substances multiply, VPNs have risen as crucial instruments for protecting online security and accessing restricted content. Be that as it may, the powerlessness of conventional VPN conventions to discovery and blocking requires nonstop development to guarantee vigorous security against meddlesome measures forced by ISPs, arrange chairmen, and administrative bodies.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest in this work.

Data Availability Statement

Data available on request from the corresponding author upon reasonable request.

Author Contribution Statement

Mohammad Shehab: Conceptualization, Methodology, Validation, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration. **Lial Raja Alzabin:** Conceptualization, Methodology, Formal analysis, Resources, Writing – review & editing, Visualization.

References

[1] Iqbal, M., & Riadi, I. (2019). Analysis of security Virtual Private Network (VPN) using openVPN. *International Journal of Cyber-Security and Digital Forensics, 8*(1), 58–65.

[2] Kashif, M., & Kalkan, K. (2024). EPIoT: Enhanced privacy preservation based blockchain mechanism for internet-of-things. *Computer Networks, 238,* 110107. https://doi.org/10.1016/j.comnet.2023.110107

[3] Al-Zabin, L. R., Al-Wesabi, O. A., Al Hajri, H., Abdullah, N., Khudayer, B. H., & Al Lawati, H. (2023). Probabilistic detection of indoor events using a wireless sensor network-based mechanism. *Sensors, 23*(15), 6918. https://doi.org/10.3390/s23156918

[4] Alice, Bob, Carol, Beznazwy, J., & Houmansadr, A. (2020). How China detects and blocks Shadowsocks. In *Proceedings of the ACM Internet Measurement Conference,* 111–124. https://doi.org/10.1145/3419394.3423644

[5] Nan, Z., Wu, T., Zhang, Y., & Xiao, M. (2020). Shadowsocks traffic identification based on convolutional neural network. In *International Conference on Information Science and Education,* 480–485. https://doi.org/10.1109/ICISE51755.2020.00109

[6] Mohd Fuzi, M. F., Mohd Alias, M. R., Kaur, N., & Abd Halim, I. H. (2021). SafeSearch: Obfuscated VPN server using Raspberry Pi for secure network. *Journal of Computing Research & Innovation, 6*(4), 93–104. https://doi.org/10.24191/jcrinn.v6i4.230

[7] Chen, H. Y., & Lin, T. N. (2021). The challenge of only one flow problem for traffic classification in identity obfuscation environments. *IEEE Access, 9,* 84110–84121. https://doi.org/10.1109/ACCESS.2021.3087528

[8] Paillisse, J., Barcia, A., Lopez, A., Rodriguez-Natal, A., Maino, F., & Cabellos, A. (2021). A control plane for WireGuard. In *International Conference on Computer Communications and Networks,* 1–8. https://doi.org/10.1109/ICCCN52240.2021.9522315

[9] Mackey, S., Mihov, I., Nosenko, A., Vega, F., & Cheng, Y. (2020). A performance comparison of WireGuard and OpenVPN. In *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy,* 162–164. https://doi.org/10.1145/3374664.3379532

[10] Park, P., Ryu, H., Hong, G., Yoo, S., Park, J., & Ryou, J. (2015). A service protection mechanism using VPN GW hiding techniques. In *Information Science and Applications,* 1053–1062. https://doi.org/10.1007/978-3-662-46578-3_125

[11] Bansal, M., Kumar, M., Sachdeva, M., & Mittal, A. (2023). Transfer learning for image classification using VGG19: Caltech-101 image data set. *Journal of Ambient Intelligence and Humanized Computing, 14,* 3609–3620. https://doi.org/10.1007/s12652-021-03488-z

[12] Ma, Z., Mason, J., Antonakakis, M., Durumeric, Z., & Bailey, M. (2021). What's in a name? Exploring CA certificate

control. In *Proceedings of the 30th USENIX Security Symposium,* 4383–4400.

[13] Nelson, R., Shukla, A., & Smith, C. (2020). Web browser forensics in Google Chrome, Mozilla Firefox, and the tor browser bundle. In X. Zhang & K. R. Choo (Eds.), *Digital forensic education: An experiential learning approach* (pp. 219–241). Springer. https://doi.org/10.1007/978-3-030-23547-5_12

[14] Cho, J. Y., Sergeev, A., & Zou, J. (2019). Securing ethernet-based optical fronthaul for 5G network. In *Proceedings of the 14th International Conference on Availability, Reliability and Security,* 106. https://doi.org/10.1145/3339252.3341484

[15] AlZabin, L. R., Firdouse, M. J., & Khudayer, B. H. (2024). A literature survey on event detection for indoor environment using wireless sensor network. In *Advanced Engineering, Technology and Applications: Second International Conference,* 38–56. https://doi.org/10.1007/978-3-031-50920-9_4

[16] Yu, F. Y., & Sung, S. (2016). A mixed methods approach to the assessor's targeting behavior during online peer assessment: Effects of anonymity and underlying reasons. *Interactive Learning Environments, 24*(7), 1674–1691. https://doi.org/10.1080/10494820.2015.1041405

[17] Santamaría, L., Nieto, M. J., & Rodríguez, A. (2021). Failed and successful innovations: The role of geographic proximity and international diversity of partners in technological collaboration. *Technological Forecasting and Social Change, 166,* 120575. https://doi.org/10.1016/j.techfore.2021.120575

[18] Liu, L., Yu, H., Yu, S., & Yu, X. (2022). Network traffic obfuscation against traffic classification. *Security and Communication Networks, 2022*(1), 3104392. https://doi.org/10.1155/2022/3104392

[19] Emmanuel, O. I., Ayodele, A. A., Adebiyi, A. M., & Osang, B. F. (2021). Windows firewall bypassing techniques: An overview of HTTP tunneling and Nmap evasion. In *Computational Science and Its Applications: 21st International Conference,* 546–556. https://doi.org/10.1007/978-3-030-87013-3_41

[20] Pudelko, M., Emmerich, P., Gallenmüller, S., & Carle, G. (2020). Performance analysis of VPN gateways. In *IFIP Networking Conference (Networking),* 325–333.

[21] Langenberg, B., Janczyk, M., Koob, V., Kliegl, R., & Mayer, A. (2023). A tutorial on using the paired *t* test for power calculations in repeated measures ANOVA with interactions. *Behavior Research Methods, 55*(5), 2467–2484. https://doi.org/10.3758/s13428-022-01902-8

[22] Chen, S., Qian, Y., Zang, X., & Peng, R. (2017). A proxy based connection mechanism for hybrid cloud virtual network. In *IEEE 3rd International Conference on Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS*), 80–85. https://doi.org/10.1109/BigDataSecurity.2017.55

[23] Jiang, X., Shokri-Ghadikolaei, H., Fodor, G., Modiano, E., Pang, Z., Zorzi, M., & Fischione, C. (2019). Low-latency networking: Where latency lurks and how to tame it. *Proceedings of the IEEE, 107*(2), 280–306. https://doi.org/10.1109/JPROC.2018.2863960

[24] Abbas, H., Emmanuel, N., Amjad, M. F., Yaqoob, T., Atiquzzaman, M., Iqbal, Z., ..., & U. Ashfaq, (2023). Security assessment and evaluation of VPNs: A comprehensive survey. *ACM Computing Surveys, 55,* 1–47. https://doi.org/10.1145/3579162

[25] Common, M. F. (2023). Beyond the usual suspects: A taxonomy of social media regulations in countries with human rights issues. *International Review of Law, Computers & Technology, 37*(1), 1–28. https://doi.org/10.1080/13600869.2022.2043093

[26] Eichensehr, K. E., & Hwang, C. (2023). National security creep in corporate transactions. *Columbia Law Review, 123*(2), 549–614.

How to Cite: Shehab, M., & Alzabin, L. R. (2024). Evaluating the Effectiveness of Stealth Protocols and Proxying in Hiding VPN Usage. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewJCCE42023642