# CONTENTS

# LIST OF USED ABBREVIATIONS

**VPN** - Virtual Private Network

# INTRODUCTION

In an age when digital communications plays an vital role in modern society, ensuring the confidentiality and integrity of network communications has become crucial. The emergence of virtual private networks (VPNs) as a method of securing and privatizing digital communications on the public Internet has been a significant development in this direction. Because of the growing popularity of virtual private networks (VPNs), governmental agencies and corporate network administrators have increased their efforts to identify and block these encrypted connections. The result has been an arms race between organizations seeking to monitor, control, or censor Internet traffic and VPN service providers competing for the privacy of their users. The implementation of VPN obfuscation, a progressive collection of technologies capable of disguising VPN traffic as routine Internet operations, is central to this dispute. This obfuscation allows unrestricted access to the global digital environment.

VPNs were initially implemented as a simple way to establish secure network connections across the insecure infrastructure of the public Internet. However, the use of VPN technology eventually surpassed the scope of corporate applications. Private users are increasingly adopting virtual private networks (VPNs) for their own benefit, owing to the potential for enhanced privacy, circumvention of surveillance, circumvention of content geo-restrictions, and protection against cyber threats. In response, efforts to undermine the effectiveness of virtual private networks (VPNs) have increased. These initiatives include corporate firewall policies, government censorship initiatives such as China's Great Firewall, and anti-VPN measures implemented by content providers (El-Maghraby et al. 2017).

The proliferation of anti-VPN initiatives has sparked the emergence of a complex area of cybersecurity that uses data packet signatures to distinguish VPN connections. In response, the VPN obfuscation movement has developed a number of countermeasures. As a recent example, we have the Geneva algorithm which employs genetic algorithms to generate dynamic, packet-manipulation-based evasion strategies, providing a new take on DPI evasion (Bock et al. 2019).

Steganography can also be utilized in VPN obfuscation. This method provides a way around DPI systems by embedding VPN traffic inside regular data streams. Steganography enables regular web traffic, like audio or video streams, to conceal VPN packets, making it difficult for DPI tools to discern between encrypted and regular traffic (Kundur & Ahsan 2003). The effectiveness and subtlety of this method are assessed, offering insights into its limitations and useful applications in different network environments.

Another way of obfuscating VPN traffic is through the application of port switching. To avoid detection, a VPN server is configured to use non-standard ports, which can assist in getting around simple DPI systems that keep an eye on popular VPN ports.

Another way of providing VPN obfuscation is the integration of encrypted proxy tunneling software like Shadowsocks and Stunnel. It can be used to make VPN traffic look like HTTPS traffic (Clowwindy et al. n.d.).

All of these methods, excluding port switching, bring with them a trade-off of in connection speed and throughput, though of varying degrees.

The thesis begins with a comprehensive overview of VPN technology and then describes the various use cases for VPNs as well as the fundamental principles underlying their operation. It then describes the techniques used to detect VPN traffic. The following is a comprehensive examination of various obfuscation methods and their adaptation to evolving VPN traffic detection strategies. The goal of this analysis is to provide insight into VPN detection methodologies and obfuscation techniques through experimentation, qualitative assessment, and technical proficiency in the process developing a methodology by which one can consider selecting an obfuscation method in real-life scenarios.

# 1. BACKGROUND

## 1.1. Deep packet inspection

A type of network packet filtering known as Deep Packet Inspection (DPI) looks at a packet's data portion as well as frequently its header as it passes an inspection point. DPI examines the packet's data payload in depth as opposed to conventional packet filtering, which simply looks at the header section, allowing for more complex packet decision-making. DPI can now detect, identify, classify, reroute, or prevent packets containing particular data or code payloads thanks to this sophisticated technique.

Due to its great versatility, DPI technology is employed in many different contexts, such as traffic management, censorship, eavesdropping, and network security. It is an essential tool for internet service providers and regulatory bodies since it can identify and manage apps using the network even in the face of encryption and port-hopping schemes.

### 1.1.1. DPI in Relation to VPNs

DPI is important when it comes to VPNs (Virtual Private Networks). In order to protect privacy and get around censorship or geographical limitations, VPNs usually encrypt data. Nonetheless, DPI can be used to examine encrypted packet metadata, including timing, size, destination, and protocol. This makes it possible to identify VPN activity even when the content is encrypted.

Certain DPI techniques can detect the signatures of the encryption protocols used by VPNs, allowing them to differentiate between conventional and VPN traffic. This capability is essential in situations when the use of VPNs is prohibited or closely watched, like in nations with severe internet censorship.

### 1.1.2. DPI's Challenges for VPNs

VPN technologies have substantial hurdles due to the efficacy of DPI:

- **Detection and Blocking**: If Advanced DPI detects that a VPN is being used, it has the ability to either block or limit data, making the VPN useless for getting around censorship or geographical restrictions.

- **Avoiding Encryption**: Although DPI is unable to decrypt data, it can identify and potentially block VPN services based on educated estimates about the encrypted traffic's nature.

- **Adaptive Countermeasures**: VPN service providers are compelled to constantly modify and introduce fresh methods to avoid being detected by DPI, resulting in a never-ending game of cat and mouse between VPN providers and DPI-using companies.

### 1.1.3. Case Studies

- **The Great Firewall of China**: China's Great Firewall is among the most well-known applications of DPI technology. Among other censoring tools, it uses advanced DPI techniques to identify and restrict VPN connections. VPN service providers frequently need to improve their techniques on a regular basis to avoid being detected.

- **Iran's Internet Censorship**: Especially during political turmoil, Iran's government use DPI to monitor and regulate internet traffic, including the detection and blocking of VPN usage.

- **Corporate Network Management**: By keeping an eye out for unauthorised VPN use that might go around corporate security measures, DPI is utilised in a business context to guarantee security and compliance.

- **Russia's Telegram Ban**: Using DPI, Russia tried to ban the messaging service Telegram. Telegram, however, circumvented this restriction using a variety of strategies, including VPNs, illustrating the continuous conflict between DPI implementation and VPN evasion approaches.

In conclusion, DPI not only poses a serious threat to VPN technologies but also propels the ongoing development of VPN obfuscation strategies including port switching, network steganography, and sophisticated tunnelling methods like Geneva, Shadowsocks, and Stunnel.

## 1.2. OpenVPN identification

## 1.3. Packet manipulation

## 1.4. Protocol obfuscation

# 2. EXPERIMENTATION

## 2.1. Testbed

## 2.2. Port switching

## 2.3. Steganography

## 2.4. Geneva

## 2.5. Encryption tunneling

# CONCLUSION

# REFERENCES

1. Bock, K., Hughey, G., Qiang, X. & Levin, D. (2019), Geneva: Evolving censorship evasion strategies, pp. 2199–2214.

2. Clowwindy, Madeye & Max, L. (n.d.), ‘Shadowsocks’.
   **URL:** *http://www.shadowsocks.org/*

3. El-Maghraby, R. T., Abd Elazim, N. M. & Bahaa-Eldin, A. M. (2017), A survey on deep packet inspection, *in* ‘2017 12th International Conference on Computer Engineering and Systems (ICCES)’, pp. 188–197.

4. Kundur, D. & Ahsan, K. (2003), ‘Practical internet steganography: Data hiding in ip’.