OMAR'S THESIS

by

OMAR LOUDGHIRI

Submitted in partial fulfillment of the requirements for the degree of
Master's of Science in Computer Science

Department of Computer Science and Data Science

CASE WESTERN RESERVE UNIVERSITY

August, 2024

CASE WESTERN RESERVE UNIVERSITY

SCHOOL OF GRADUATE STUDIES

We hereby approve the thesis/dissertation of

Omar Loudghiri

candidate for the degree of **Master's of Science in Computer Science**[1].

Committee Chair

An Wang

Committee Member

Mark Allman

Committee Member

Vincenzo Liberatore

Committee Member

Mehmet Koyuturk

Date of Defense

July 10th, 2024

[1] We also certify that written approval has been obtained for any proprietary material contained therein.

DEDICATION

TBD

TABLE OF CONTENTS

List of Tables vi
List of Figures vii
Acknowledgements viii
Abstract ix
Chapter I: Introduction 1
1.1 Load Balancing 1
1.2 Impact of Load Balancing on Internet Reliability 1
1.3 Areas of Study 2
Chapter II: Related Works 3
2.1 Paris Traceroute 3
2.1.1 General Introduction 3
2.1.2 Multipath Detection Algorithm (MDA) 4
2.1.3 Usage of Paris Traceroute 5
2.2 Scamper 6
2.2.1 Introduction 6
2.2.2 Scamper Features 6
2.2.3 Multipath Detection Algorithm (MDA) in Scamper 7
2.3 Classification of Load Balancing in the Internet and Multipath Classification Algorithm (MCA) 7
2.4 MDA vs MCA 8
Chapter III: Datasets 10
3.1 Alexa Top 1 Million Websites 10
3.2 Team Cymru IP to ASN List 11
Chapter IV: Data Collection 13
4.1 Discovering Load Balancers 13
Chapter V: This is the Fourth Chapter 14

Chapter VI: This is the Fifth Chapter 15
Chapter VII: This is the Sixth Chapter 16
Chapter VIII: This is the Seventh Chapter 17
Chapter IX: This is the Eighth Chapter 18
Appendix A: Questionnaire 19

LIST OF TABLES

Number *Page*

3.1 BGP and ASN Information 11

LIST OF FIGURES

Number *Page*

ACKNOWLEDGEMENTS

TBD

Omar’s Thesis

Abstract

by

OMAR LOUDGHIRI

TBD

Chapter 1

INTRODUCTION

1.1 Load Balancing

Load balancing is a key network management technique that distributes traffic across multiple servers, preventing any single server from becoming overwhelmed. Originally developed as network-based hardware, load balancing now plays a crucial role in modern infrastructure by ensuring high availability, scalability, security, and performance.

Applications today must handle millions of simultaneous sessions. Load balancers dynamically distribute traffic across servers with duplicate data, ensuring reliable and fast data delivery. This process also provides redundancy; if a server fails, traffic is redirected to maintain continuous access.

Load balancing enhances security by minimizing attack surfaces and rerouting traffic if a server is compromised.

It also optimizes performance by managing resource use and traffic spikes. Various algorithms, such as round-robin and least connections, help distribute traffic based on real-time conditions.

The goal of this project is to measure load balancing behavior on the Internet and map the presence of load balancers worldwide. This will enhance our understanding of their impact on network performance and security.

1.2 Impact of Load Balancing on Internet Reliability

Load balancing significantly enhances the reliability of the Internet by distributing traffic across multiple servers or paths. This helps prevent any single point of failure, manage high traffic volumes, and ensure continuous availability of services.

Effective load balancing reduces latency, avoids downtime, and ensures smooth data delivery, contributing to a better user experience.

The primary motivation for this project was to explore how load balancing impacts Internet reliability. Understanding this impact is crucial, as load balancing directly affects the network's ability to handle failures, traffic spikes, and varying load conditions. Despite its importance, the extent of load balancing's contribution to Internet reliability has not been extensively quantified.

This research aims to measure and analyze the role of load balancing in maintaining Internet reliability. By mapping the global presence of load balancers and characterizing their behavior, we seek to provide a clearer picture of their impact on network resilience. Using tools like the Multipath Detection Algorithm (MDA), we will quantify how load balancing affects network performance.

In summary, load balancing is key to Internet reliability, and this project aims to quantify its significance.

1.3 Areas of Study

Chapter 2

RELATED WORKS

2.1 Paris Traceroute

2.1.1 General Introduction

The traditional model of the Internet assumes a single path between a pair of end-hosts. However, modern commercial routers often include load balancing capabilities, creating multiple active paths between hosts. This shift challenges the conventional single-path assumption used by many Internet applications, network simulation models, and measurement tools.

In their paper *Measuring Load-balanced Paths in the Internet*, Brice Augustin, Timur Friedman, and Renata Teixeira from LIP6 at Université Pierre et Marie Curie present a comprehensive study on load-balanced paths. They highlight the significance of recognizing load balancing in contemporary networking by demonstrating how it affects traffic distribution and path diversity.

The authors enhance a traceroute-like tool called *Paris traceroute*, designed to find all paths between a pair of hosts. Their methodology involves identifying load-balancing routers and characterizing the load-balanced paths. By conducting measurements from 15 sources to over 68,000 destinations, their study reveals that the traditional single-path concept no longer holds. They found that 39% of source-destination pairs traverse a load balancer, and this percentage rises to 70% when considering paths between a source and a destination network.

Their work contributes significantly to understanding Internet path diversity by:

1. Developing Paris traceroute's Multipath Detection Algorithm (MDA) to find all paths from a source to a destination under different types of load balancing.

2. Characterizing the load-balanced paths in terms of length, width, and asymmetry.

3. Establishing a methodology to measure round-trip times (RTTs) of load-balanced paths, considering delays on both forward and return paths.

This study underscores the necessity for the research community to reconsider the concept of a single Internet path and highlights the importance of accurately measuring and understanding load-balanced paths. The insights gained from this work are critical for developing more realistic network models and improving the design and reliability of Internet applications.

2.1.2 Multipath Detection Algorithm (MDA)

The Multipath Detection Algorithm (MDA) is a key component of Paris traceroute, designed to identify and trace multiple load-balanced paths between a source and a destination. Traditional traceroute tools often fail to detect load balancing because they assume a single path. In contrast, MDA systematically discovers all paths by varying flow identifiers in probe packets.

The MDA operates hop-by-hop, sending probes to identify all interfaces at each hop. For a given interface r at hop $h-1$, MDA generates several flow identifiers to ensure probes reach r. It then sends these probes one hop further to discover the next-hop interfaces $s_1, s_2, \ldots, s_n$.

To determine the number of probes k needed to discover all paths with a high degree of confidence, MDA assumes r is part of a load balancer that splits traffic evenly across n paths. If fewer than n interfaces are found, MDA stops. Otherwise, it increases n and sends additional probes to test the hypothesis.

To identify whether a load balancer uses per-packet or per-flow balancing, MDA sends probes with a constant flow identifier. If responses come from multiple interfaces, it indicates per-packet balancing. If all responses come from the same interface, it suggests per-flow balancing. MDA uses statistical methods to ensure a high level of confidence (typically 95

For instance, to reject the hypothesis of $n = 2$ with 95% confidence, MDA sends $k = 6$ probes. If load balancing across up to 16 interfaces is suspected, MDA may send up to $k = 96$ probes to ensure all paths are discovered. This process allows MDA to effectively enumerate all paths and classify the type of load balancing in use.

2.1.3 Usage of Paris Traceroute

The paper by Augustin, Friedman, and Teixeira is one of the few studies that actively measures the presence and behavior of load balancers in the Internet.

Building on the foundational work of Augustin et al., my research aims to further explore the presence and behavior of load balancers in the Internet. By leveraging Paris traceroute and its MDA, I will conduct extensive measurements to map the global distribution of load balancers and analyze their impact on network performance and reliability.

This study will add to the existing knowledge by:

- Expanding the scope of measurement to include a more diverse set of source-destination pairs.
- Investigating the effects of load balancing on different types of network traffic and applications.

2.2 Scamper

2.2.1 Introduction

Packet probing experiments capture simple measurements—typically delay, loss, reordering, and topology—that provide valuable insights into the structure and behavior of the Internet. For instance, early studies on packet size and delay led to improvements in the TCP RTO algorithm. As the Internet has grown, measuring it has become more complex, both technically and methodologically. Over the past decade, researchers have developed and operated many large-scale Internet measurement platforms, each involving significant software development.

In 2005, facing funding challenges, the Internet measurement community organized a workshop to plan a collaborative, community-oriented network measurement infrastructure. The workshop report highlighted the need for better organization of large-scale measurements.

This paper addresses a small part of this problem by focusing on building a packet-prober for large-scale measurements and well-defined data archiving. A packet-prober should simplify the coordination of measurements, provide APIs for operating system differences, offer accurate timing information, and produce detailed, easy-to-process output. This approach helps researchers avoid system programming and administrative challenges, allowing them to implement new measurement techniques and focus on analysis and validation.

2.2.2 Scamper Features

Scamper is a powerful packet-prober designed to support large-scale Internet measurement. It includes feature-rich implementations of traceroute, ping, MDA traceroute, four alias resolution techniques, Sting, and parts of TBIT.

2.2.3 Multipath Detection Algorithm (MDA) in Scamper

Scamper implements the Multipath Detection Algorithm (MDA) described by Augustin et al. to infer all interfaces visited between a source and destination in a per-flow load-balanced Internet path. The MDA achieves this by deliberately varying the flow identifier that a router may compute when load balancing. Probes with different flow identifiers may take different paths, thereby revealing different parts of the forward IP path.

In addition to the ICMP and UDP methods originally implemented by Augustin et al., which vary the ICMP checksum and UDP destination port values, Scamper implements a UDP method that varies the source port instead of the destination port. This prevents the probes from appearing as a port scan and enables probing past firewalls that block UDP probes to ports above the usual range used by traceroute. Scamper also implements TCP methods that vary the flow identifier by changing either the source or destination port, depending on the user's choice.

Scamper's MDA traceroute functionality was used to conduct scheduled data collection throughout this project.

2.3 Classification of Load Balancing in the Internet and Multipath Classification Algorithm (MCA)

Recent advances in programmable data planes, software-defined networking, and the adoption of IPv6 have enabled more complex load balancing strategies. Almeida et al. introduced the Multipath Classification Algorithm (MCA), which enhances the existing Multipath Detection Algorithm (MDA). While MDA systematically varies probes' flow identifiers to identify load-balanced paths, MCA extends this by considering arbitrary combinations of bits in the packet header for load balancing.

Key contributions of MCA include:

- **Enhanced Classification:** MCA identifies the specific bits in the packet header used by load balancers, providing a more detailed and accurate classification than MDA, which primarily varies transport port numbers and the ICMP checksum.

- **Efficiency Optimizations:** The researchers developed optimizations to reduce the probing cost. MCA achieves this with a minimal increase in the number of probes, only 34% higher than MDA, while maintaining accuracy.

- **Comprehensive Measurements:** Through large-scale measurement campaigns, MCA characterizes load balancing on both IPv4 and IPv6 Internet paths. The results show that load balancing is more prevalent and sophisticated than previously reported.

The study revealed that 74% of IPv4 and 56% of IPv6 routes traverse at least one load balancer. Additionally, 23% of IPv4 and 18% of IPv6 load balancers have three or more next hops, indicating complex load balancing configurations.

Building on this work, part of our research uses MCA to map the global presence of load balancers and analyze their impact on network performance and reliability.

2.4 MDA vs MCA

While MCA offers significant improvements in identifying and classifying load balancers by considering a broader range of packet header bits, it is less accessible for fine-tuning and practical use. For my research, I opted to use MDA due to its better integrability with existing tools and faster runtime performance. MDA's established methodologies and ease of implementation make it a more practical choice for large-scale measurements. The decision to use MDA is further justified by its compatibility with current infrastructure and the ability to conduct measurements efficiently. Detailed explanations of MDA's integration and performance in my study will be provided in a later section of this document.

Chapter 3

DATASETS

3.1 Alexa Top 1 Million Websites

The Alexa Top 1 Million Websites list was utilized as the primary dataset for this research. The latest update to this list was in February 2023, ensuring its relevance at the start of the study. The Alexa list is renowned for its accuracy in ranking the most visited websites globally, making it an ideal source for identifying widely used routes on the Internet.

Alexa rank employs a proprietary methodology that combines visitor engagement and estimated traffic to generate the ranking list. Data is analyzed over the past three months, considering factors such as unique daily visitors and page views. Unique visitors are defined as the number of distinct Alexa users visiting a site on a single day, while page views represent the total number of URL requests generated by Alexa users for a site. The Alexa Toolbar, available as a browser extension for Chrome, Internet Explorer, and Firefox, facilitates data collection by recording URLs and IP addresses, sending traffic data to Alexa's central server.

The Alexa ranking is particularly useful for this research as it includes a diverse range of popular websites. This diversity is crucial for finding load balancers on heavily trafficked routes, allowing for a comprehensive analysis of load balancing behavior across different types of web traffic and services. By focusing on these high-traffic websites, the study can better capture the impact of load balancing on Internet reliability and performance.

It should be noted that while Alexa provides reliable rankings for the top 100,000 websites, its accuracy diminishes for lower-ranked sites due to limited data. This limitation is not heavily impacting our data collection as we are taking 2000 random samples from those top 100,000 websites for different stages of the data collection.

The domain names from the Alexa list are then resolved into the most current IP addresses using the DNS lookup tool. In the context of this project, this ensures that the analysis is based on up-to-date routing information, allowing for accurate identification and characterization of load balancers on the most heavily trafficked Internet routes.

3.2 Team Cymru IP to ASN List

For this project, the Team Cymru IP to ASN mapping service was utilized to resolve IP addresses to their corresponding Autonomous System Numbers (ASNs). Team Cymru provides a robust service dedicated to mapping IP numbers to BGP prefixes and ASNs, based on BGP feeds from over 50 peers, updated at four-hour intervals.

This service supports multiple query methods, including WHOIS (TCP 43), DNS (UDP 53), and HTTPS (TCP 443). Here is an example of an entry with definitions of the fields:

Field	**Example**
BGP Origin ASN	23489
BGP Peer ASN	199.88.100.1
BGP Prefix	199.88.100.0/24
Prefix Country Code (assigned)	US
Prefix Registry (assigned)	arin
Prefix Allocation Date	1994-03-28
ASN Country Code (assigned)	US
ASN Registry (assigned)	arin
ASN Allocation Date	1994-03-28
ASN Description	MARINK12, US

Table 3.1: BGP and ASN Information

It is important to note that the IP to ASN mapping service is not a GeoIP service. The country code, registry, and allocation date are based on data from regional registries, such as ARIN, RIPE, AFRINIC, APNIC, and LACNIC. As such, the accuracy of this information depends on the data present in the RIR databases.

In the context of this project, the Team Cymru service was essential for obtaining accurate WHOIS lookup results and mapping IP addresses to their respective ASNs. My advisor, Professor Mark Allman, automated a script that pulls all their current IP to ASN mappings every month. This list was used to cross-reference the IPs identified as load balancers, their next hop, and their destination IPs. This comprehensive cross-referencing provided detailed insights into the load balancers discovered.

Chapter 4

DATA COLLECTION

4.1 Discovering Load Balancers

The data collection process for this research involved using a Python script to automate the execution of the Paris traceroute tool and process its output. The script was designed to systematically gather information about network routes and load balancers.

The process begins by reading the top 2000 domains from the Alexa Top 1 Million Websites list, which is stored in a CSV file. This ensures that the analysis focuses on high-traffic websites that are likely to traverse significant portions of the Internet's infrastructure.

For each domain, the script runs the Paris traceroute tool using the Multipath Detection Algorithm (MDA). The traceroute is executed with a timeout of 40 seconds to prevent any hanging processes. The output from the traceroute is captured and saved to a file in a designated output directory. If a timeout or error occurs, appropriate messages are logged to keep track of any issues during execution.

Once the traceroute output is obtained, the script parses the data using regular expressions to extract relevant IP addresses and paths. This parsed data is then organized into a JSON structure, mapping each source IP to its multiple destination IPs. This structure is essential for analyzing the network paths and identifying load balancers.

In addition to the traceroute data, the script utilizes the Team Cymru IP to ASN mapping service to resolve IP addresses to their corresponding Autonomous System Numbers (ASNs). This list was used to cross-reference the IPs identified as load balancers, as well as their next hops and destination IPs.

Chapter 5

THIS IS THE FOURTH CHAPTER

Chapter 6

THIS IS THE FIFTH CHAPTER

Chapter 7

THIS IS THE SIXTH CHAPTER

Chapter 8

THIS IS THE SEVENTH CHAPTER

Chapter 9

THIS IS THE EIGHTH CHAPTER

Appendix A

QUESTIONNAIRE