Affecting IP traceback with recent Internet topology maps

Olawale Abiodun Martins

Iowa State University

Follow this and additional works at: https://lib.dr.iastate.edu/rtd

Recommended Citation
https://lib.dr.iastate.edu/rtd/19175

This Thesis is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Retrospective Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.
Affecting IP traceback with recent Internet topology maps

by

Olawale Abiodun Martins

A thesis submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Co-majors: Computer Engineering; Information Assurance

Program of Study Committee:
Thomas E. Daniels, Co-major Professor
Yong Guan, Co-major Professor
Tzee-Ming Huang

Iowa State University
Ames, Iowa
2005
Graduate College
Iowa State University

This is to certify that the master’s thesis of

Olawale Abiodun Martins

has met the requirements of Iowa State University

Signatures have been redacted for privacy
DEDICATION

To Jesus Christ – My raison d’être.
TABLE OF CONTENTS

LIST OF FIGURES .................................................................................................................. v

LIST OF TABLES ..................................................................................................................... vi

ACKNOWLEDGEMENTS ........................................................................................................ vii

ABSTRACT ........................................................................................................................... viii

CHAPTER 1. INTRODUCTION ............................................................................................ 1

1.1 Thesis Statement ........................................................................................................ 1
1.2 Approach ..................................................................................................................... 2
1.3 The Need for IP Traceback ....................................................................................... 3

CHAPTER 2. LITERATURE REVIEW ................................................................................. 7

2.1 Past Work .................................................................................................................... 7
2.2 Motivation .................................................................................................................. 14

CHAPTER 3. PRESENTATION AND ANALYSIS OF INTERNET MAPS ....................... 16

3.1 Internet Topology Maps .......................................................................................... 16
3.2 Definitions ............................................................................................................... 23
3.3 Statistical Analysis of CAIDA Data ....................................................................... 24
3.4 Statistical Analysis of Rocketfuel Data .................................................................. 38
3.5 Comparisons with RIPE’s RIS Data ...................................................................... 41

CHAPTER 4. PROPOSAL AND EVALUATION OF TRACEBACK SCHEMES ............ 44

4.1 Underlying Concept to Proposed DPM Schemes ................................................... 44
4.2 Proposed Schemes and Evaluations ........................................................................ 48
4.3 Security Issues ........................................................................................................ 58
4.4 Comparison of GUM to other DPM Schemes ....................................................... 59

CHAPTER 5. CONCLUSIONS AND FUTURE WORK .................................................. 62

5.1 Conclusions ............................................................................................................. 62
5.2 Future Work ............................................................................................................. 62

APPENDIX A. LOCATION AND CURRENT STATUS OF CAIDA MONITORS ....... 64

APPENDIX B. LIST OF ISP’S MAPPED BY ROCKETFUEL ........................................ 65

REFERENCES ....................................................................................................................... 66
LIST OF FIGURES

Figure 1. Schematic of IP Traceback Categories ....................................................... 8
Figure 2. Sample Raw Data from CAIDA's Skitter Tool........................................... 21
Figure 3. AS Node Degree Frequency .................................................................... 27
Figure 4. AS Node Degree Distribution ................................................................. 28
Figure 5. AS Path Length Frequency .................................................................... 31
Figure 6. AS Path Length Distribution ................................................................. 31
Figure 7. Comparison of AS Path Length Distribution for Select Monitor Locations ... 32
Figure 8. AS Unique-Neighbor Degree Frequency .............................................. 34
Figure 9. AS Unique-Neighbor Degree Distribution ............................................. 34
Figure 10. Frequency of Number of Transit AS per Path ...................................... 36
Figure 11. Cumulative Distribution of Number of Transit AS per Path ................. 36
Figure 12. Frequency of Number of Initial Origin AS in a Path ......................... 37
Figure 13. Distribution of Number of Initial Origin AS in a Path ....................... 37
Figure 14. POP Node Degree Frequency ............................................................. 39
Figure 15. POP Node Degree Distribution .......................................................... 40
Figure 16. POP-Level View of the Internet .......................................................... 45
Figure 17. AS-Level View of the Internet ............................................................. 40
Figure 18. Frequency of Sum of Ceiling of Bits Required to Encode Paths .......... 49
Figure 19. Distribution of Sum of Ceiling of Bits Required to Encode Paths ......... 50
Figure 20. Unique-Neighbor: Frequency of Sum of Ceiling .............................. 52
Figure 21. Unique-Neighbor: Distribution of Sum of Ceiling ............................ 53
Figure 22. Fields in the Globally Unique Marks Scheme ....................................... 55
LIST OF TABLES

Table 1. Statistics of AS Node Degree ................................................................. 29
Table 2. Mean AS Path Length Per Monitor ........................................................ 33
Table 3. Statistical Values for Transit AS Indices ............................................. 38
Table 4. Frequency of POP Path Length in Sample Data .................................. 41
Table 5. Comparison CAIDA and RIPE RIS Data ............................................. 42
Table 6. Partial Deployment Measurements for GUM ........................................ 58
ACKNOWLEDGEMENTS

I wish to express my profound gratitude to everyone who made the completion of this project and my program successful. You are all stakeholders in this deeply grateful entity.

I thank God Almighty for His love, enablement, and provision. Were it not for Most High, I would be neither here nor there, and so I praise and thank Him always.

I also thank all members of my family. I am probably one of the few lucky ones out there blessed with two wonderful pairs of parents and I really appreciate and thank each one for the constant labor of love. I thank my brother and sisters, Jide, Dayo, Nike, and Ronke, including their respective families; and also Toun, Titi, and Funke. I thank all the cousins I have been blessed with, Tade, Muyiwa, Lola, Damola, Bode, and so many others, as well as a host of uncles and aunts too numerous to mention. You are all loved.

I thank Tom Daniels. I guess many wonder why it is that all your students tell whoever asks and even those who don’t, that they have the best major professor anyone could ask for. The reason is simple – it is true. I really appreciate your guidance, patience, and support. I guess now is a better time than ever to confess that I sometimes leave your office, after a brain-storming session, wondering if you had not missed a step or two, only to realize as I try to implement, that you were simply working that step or two ahead. Again, thank you so much.

I thank my other professors including my committee members, Dr. Guan and Dr. Huang. I also thank my colleagues, Wei, Tang, Jianqiang, Ben, Greg, Christy, and several other classmates and friends. I thank the always cheerful and ready to assist, Pam Myers. James Davis, thank you.

Finally I thank all my friends, not least, the ones I made in Ames. Ev Cochrane Senior, thank you so much and continue to rest in peace, Ev Junior – always there, Jennifer and her family, Ejirofor, Pastor Pilcher and all members of First Assembly of God in Ames. I thank Debola and the rest of the home crowd, including my African Fellowship brothers. I thank you Pastor Kris – you make His word so real. Finally I thank my best friend Arike, out of sight maybe, but never out of mind.
ABSTRACT

Computer network attacks are on the increase and are more sophisticated in today’s network environment than ever before. One step in tackling the increasing spate of attacks is the availability of a system that can trace attack packets back to their original sources irrespective of invalid or manipulated source addresses. IP Traceback is one of such methods, and several schemes have already been proposed in this area. Notably though, no traceback scheme is in wide use today due to reasons including a lack of compatibility with existing network protocols and infrastructure, as well as the high costs of deployment.

Recently, remarkable progress has been made in the area of Internet topology mappings and more detailed and useful maps and metrics of the Internet are being made available to the corporate and academic research communities. This thesis introduces a novel use of these maps to influence IP Traceback in general, and packet marking schemes in particular. We note that while other schemes have previously taken advantage of such maps, most of these have viewed the maps from the available router node level. We take a novel router-aggregation node view of the Internet and explore ways to use this to make improvements to packet marking schemes and solving the problem of the limited space available in the current IP header for marking purposes. We evaluate our proposed schemes using real network paths traversed by several traceroute packets from diverse sources and to various destinations, and compare our results to other packet marking schemes. Finally, we explore the possibility of partial deployment of one of our schemes and estimate the probability of success at different stages of deployment.
CHAPTER 1. INTRODUCTION

In this chapter, we define the problem in general and give a high level description of our approach to the problem. We also discuss the importance of IP Traceback and its need in today’s network environment.

1.1 Problem Statement

IP Traceback (IPT) is a method that enables the proper identification of the source of a packet on a network and may at the same time provide the full or partial path reconstruction of that packet as it traverses the network. For a number of reasons which will be addressed later in this chapter, there is a need to find out where a packet came from, which path it might have taken, and who or what may have been involved or used in placing that packet on a network. To this end, various IP Traceback schemes, and specifically of interest in our work, packet marking schemes, have been proposed. However, while many of these appear promising, a key restraining element in the adaptability of such schemes has been the high demand in resources required to achieve many of these and as a consequence, there is a lack of compatibility with existing network protocol and infrastructure. Such demanding resources include scheme-specific ones such as the high storage requirements of packet logging schemes, and the large and unavailable number of bits needed to encode traceback information in packet marking schemes; and also other non-trivial requirements common to most schemes, such as the need for wide and costly deployments.

We introduce the problem of finding a packet marking IPT scheme that can trace back a single packet to its network origin and provide full or partial path reconstruction, while
minimizing costs and computing overhead with respect to the packet as well as nodes traversed, and also maintaining backward compatibility with existing protocol and network infrastructure. We also require such a scheme to be robust and capable of partial deployment and thus not requiring active participation of all network nodes.

1.2 Approach

There are various approaches that can and have been used in IP traceback, and many of these can be broadly categorized under packet logging or packet marking schemes (we discuss these further in chapter 2). Depending on such criteria as storage overhead either within the packet itself or at nodes traversed, link speeds, or computational demands, among other mitigating factors; each category has its advantages and disadvantages. For example, the hash-based approach [3] is a logging method that can trace a single packet, unlike most packet marking schemes which assume a reasonably large number of packets for successful traceback. However, the same hash-based approach presents a demerit in that it computes and stores a Bloom filter digest for every packet and this comes at a high cost in terms of the storage and computational overhead when compared to marking every packet. We note though, that to date IP Traceback schemes in either category have commonly looked at traceback from a router-level view, and this is probably due to the fact that our best view of networks have mostly been at this level.

More recently however, there have been advances in topological measurements of the Internet and we now have more detailed data at different router aggregation levels such as POP (point of presence) and AS (autonomous system) levels. We examine these levels from the perspective of obtaining statistical data, relevant to and able to affect and advance IPT
towards schemes that possess both a reduced demand on resources as well as backward compatibility with current protocols and infrastructure. Like [21] we believe that gaining a better understanding of the topology of the Internet can assist us in finding better encoding schemes in packet marking for example, but even further, such knowledge can be leveraged to improve other existing IPT schemes. Thus our focus and approach is twofold: first, to examine and process current internet topology data and provide various significant details on the autonomous systems (AS) and point-of-presence (POP) orientations of the Internet which can be exploited in traceback schemes; and second, we go ahead to propose novel packet marking schemes, based on our findings, and which are capable of tracing back a single packet to its network origin and provide a partial path reconstruction while minimizing the cost and computing overhead with respect to both the packet itself as well as the nodes it traverses, required in achieving this. We evaluate our schemes on sets of real-world Internet topologies taking advantage of the same Internet mapping data, and provide results which demonstrate that our schemes are successful. Finally, we put forward one of these schemes, GUMS (Globally Unique Marks Scheme) as one that in addition possesses compatibility with the existing IPv4 header and does not require wide or full deployment. And we perform analyses to examine how our scheme performs at different levels of partial deployment.

1.3 The Need for IP Traceback

At the onset of the Internet, accountability and attribution were hardly taken into consideration. There was good reason for this though; most of the hosts and networks that formed the first inter-networks were owned by individuals and/or organizations that were known to one another and so intentional hostile actions hardly ever occurred and preventing
and attributing such were out of the thought radar of many at the time. Today however, with
the Internet spanning over 180 countries and with diverse individuals and organizations able
to connect at the click of a mouse, attacks can and do come from anywhere and with the
ability to equally reach anywhere within a network such as the Internet. To make matters
worse, not only can these attacks be successfully launched, but due to the stateless nature of
the Internet, they may also be cleverly disguised so that their true origins may never be
known. And the fact that this will lead to even more increased attacks is very reasonable
when one considers the report by Moore et al [59] that in a survey over a period of 3 weeks,
there were 12,000 denial-of-service attacks alone against 5,000 targets, as well as the report
in [30] on the “Attack on Internet Called Largest Ever”. Furthermore, a Riptech report in
2002 projects an annual growth of 64% for Internet attacks [64].

It is widely acknowledged that the current design of the IP protocol and its routing
mechanism does not lend itself to concrete identification of the origin of a packet. Due to its
destination oriented routing there is no provision made for the validation or verification of
the source address claimed by a packet. Furthermore and ironically, many applications and
protocols designed to aid IP network performance and effectiveness can and have been
turned around in many instances to perpetrate and mask hostile attacks. NAT, IP forwarding,
ICMP, Mobile IP, for example, all have well-meaning objectives in their design, but these
same applications and protocols in the hands of the clever but malicious user can be misused
to carry out devastating attacks that the victim may not be able to prevent or attribute. For
example, simply taking advantage of the lack of packet source address validation, attackers
can easily spoof source addresses and launch a denial-of-service attack that will be not be
correctly attributable based on the value of the source IP address; likewise since IP
forwarding in its operation maintains no audit trail, it can be employed in a data theft attack such that no useful trail is left for tracking; and similarly Mobile IP which allows a host to operate from a foreign location while maintaining its local IP address can be cleverly used to cover notorious tracks or create misleading ones; indeed the list of possibilities are many. Even more ominous is the fact that various toolkits that exploit these vulnerabilities are readily available and accessible on the Internet. Discarding and replacing all of these tools is almost unrealistic; and while finding innovative solutions to solve the problem is an ongoing challenge, there have been many proposals of systems that seek to do just that.

As noted in [3], it is widely held that systems that can reliably trace individual packets back to their sources are a first and important step in making attackers or, at least, the systems they use accountable. There are a number of significant challenges in the construction of such a tracing system, including determining which packets to trace, maintaining privacy (that is, a tracing system should not adversely impact the privacy of legitimate users), and minimizing cost (both in router time spent tracking rather than forwarding packets, and in storage used to keep information). IP Traceback is one of those methods receiving a lot of attention in this quest.

IP Traceback is still very open to many definitions but it is typically understood to be any method that enables the proper identification of the source of a packet on a network. A successful method that can allow us to take a packet (or a copy of it) and analyze it so as to find its true origin is a tool that will go a long way in restraining attacks by hitherto faceless attackers and also aid in tracking successful attacks, and IPT has steadily gained acceptance as a concept capable of doing exactly that. To counter attacks, specifically in terms of
prevention, mitigation, and attribution, IP Traceback offers respectively, restraint, ability to respond decisively, and traceback as parts of an overall solution.
CHAPTER 2. LITERATURE REVIEW

In this chapter, we take a look at past work in the field of IP Traceback, discussing the various categories and schemes and the significant advantages and limitations of each of these. We end the chapter by discussing the motivations for our research.

2.1 Past Work

In this section, we will discuss significant past work related to IP Traceback and also divide each of these into different categories and subcategories. We note that while there are a lot of individual interpretations as to how to categorize IPT schemes, the differences are usually subtle and merely academic; and more importantly the overall advantages and disadvantages of each type of schemes are typically standard in the literature.

We agree with [2] that there are two main approaches to performing IP Traceback: infrastructure (or network) schemes and end host schemes. We adopt these two as distinct categories and present further classifications within each and as shown in figure 2.1.

2.1.1 Network Based Schemes

In methods under this category, the information required to achieve traceback is either stored at different points (mostly on routers) along the path that a packet traverses or that path and usually other incidental paths are analyzed to gain information that will be used in traceback. It is this distinction that we employ to further divide network based schemes into packet logging schemes and network analysis schemes.
2.1.1.1 Packet Logging Schemes

In packet logging schemes, traceback is accomplished by requiring nodes that a packet traverses to log information about that packet in such a format that can later be queried to discover if the packet has been seen at that node. The big drawback here is the huge amount of storage that may be needed at each node especially at nodes connected to high speed links that witness a lot of traffic. One of the most definitive works in IP Traceback is the Hash-based IP Traceback scheme [3] which computes and stores a Bloom filter digest for every packet at each node. The scheme comprises a Source Path Isolation Engine (SPIE) which instead of storing whole packets, saves space by storing only computed hashes for each
packet based on the invariant parts of the IP header along with the first 8 bytes of the payload. The use of a Bloom filter was innovative in addressing the storage space problems of packet logging schemes but despite this, the requirements in terms of computation and space are still formidable. As noted in [4] “assuming a packet size of 1000 bits, a duplex OC-192 link requires 60 million hash operations to be performed every second, resulting in the use of SRAM (50ns DRAM is too slow for this) and 44GB of storage per hour, with the parameters suggested in” [3]. To resolve this, [4] went ahead to propose a packet logging based traceback scheme that is scalable to such high link speeds by sampling and logging only a small percentage of packets and then using more sophisticated techniques to achieve traceback. We note however that the approach taken by [4] loses the single packet traceback ability originally possessed by [3].

2.1.1.2 Network Analyzing Schemes

Various schemes proposed under this subcategory make use of innovative ideas that examine and analyze one or more network conditions and changes to this over some period, with the objective of achieving traceback. It is important to note that most methods discussed here typically address attack attribution; however, they can also achieve IP traceback as a part of their operation. Notable schemes that utilize network analysis are described below:

Link Testing

Cheswick and Burch [5] proposed a technique that involved first mapping the paths from the victim of a denial of service attack to all possible networks. Next, sources of network load are identified (usually hosts or networks offering the UDP chargen service) and used to send
a brief burst of load through the network tree in a manner that starts out at the victim and spreads towards the attacker. By successively loading lines or routers along this tree and away from the victim and observing the changes in the rate of invading packets at the victim, i.e. if the stream is altered when a link is loaded, this link is probably along the path from the source to the victim, and the reverse is assumed otherwise, an attack path that leads to the source of the attacking packets is traced. The fact that the knowledge of a router-level Internet topology is required as well as the possible disruption to network links makes link testing unpractical for wide usage. Also the need for the attack to be ongoing for the scheme to work places some limitations on its adaptation.

**Link Matching**

A number of schemes use the concept of matching various observable parameters on network links to find an attack path that leads to the attacker. This is the underlying concept behind the stream matching scheme [6] which proposes that by comparing and matching streams of traffic from various links that may be connected to an attack path, similarity in content can be used to trace the path to the attacker. The basic reasoning is that if an attacker forms a connection chain to the victim by using compromised hosts to reach the victim, there is certain to be a deducible similarity in parts of the contents of the links connecting the entities involved in the attack, since all pertinent traffic from the attacker is expected to pass through these links. The basic drawback here is the need for some verifiable uniqueness in the parameters employed for stream matching, as well as the assumption that all involved links can be observed for analysis. In [7] a similar concept of monitoring a site’s Internet link for analysis is also used to detect stepping stones, but unlike [6], Zhang and Paxson based their
work not on connection content but on distinctive characteristics, such as packet size and timing, of interactive traffic. And in [8], the same network monitoring approach is employed; however the distinct difference here is that two common applications that intruders use, rlogin and telnet, are focused upon to find the connection chain of an intruder and this information is used to trace back to the attack origin. The method involves setting up packet monitors at possible traffic points on the Internet to record the activities of intruders at the packet level. When a host is compromised and used as a stepping stone to access another host, a comparison of the packet logs of the intruder at that host to logs already recorded all over the Internet is carried out to find the closest match. The results of experiments in this work showed that if a deviation is small, two connections are very often in the same connection chain. While most schemes in this category may be useful in specific applications in such places as small inter-networks operating under a single authority, as IPT schemes, they rely rather heavily on a high level of cooperation between different networks, and in many cases employ means that are obtrusive to a network’s normal operations.

2.1.2 End Host Based Schemes

In the schemes under this category, the traceback state information is typically aggregated and stored at the end host. Unlike packet logging schemes, end host based schemes, do not require storage of information along network routes and while this does present a significant advantage, the challenge however, usually comes in other areas. We further divide schemes under this category into two – ICMP messaging schemes and packet marking schemes as discussed below.
2.1.2.1 Messaging Schemes

ICMP messaging is a technique that involves sending path information about a packet but separate from the packet, using dedicated ICMP messages from the node to the victim. In a method more commonly known as ITrace and proposed by Steven M. Bellovin [9], messages are sent from different intermediate nodes in a packet’s path to the expected end node depicted in the destination address. An ICMP traceback message is created when routers traversed by the packet, generate with a low probability, the message that is sent along to the destination. The victim (in the case of an attack) will receive these ICMP’s from any of the ITrace-enabled routers along the path from source to destination that reveals that router’s location. With enough traceback messages from these routers, the traffic source and path can be determined at the destination. A basic drawback of this scheme is the extra traffic it creates, which will be an issue in several cases where bandwidth is limited. Other forms of messaging, e.g. email, can also be used with the central concept of the scheme remaining the same.

2.1.2.2 Packet Marking Schemes

Distinct from the ICMP messaging scheme, packet marking schemes encode information about the path a packet traverses in the packet itself, usually in rarely-used fields within the IP header. Apart from the well-known issue of finding enough space in the current IP header in which to place traceback information, another common problem with packet marking schemes arises from the additional computational tasks placed on routers during the marking process. There are two common methods to achieve this and we discuss below:
Deterministic Packet Marking Schemes

Deterministic packet marking involves the marking of each individual packet with a node’s marking information at one or more nodes reached by the packet in transit in such a way that traceback can be realized by considering the marks on each packet. These marks are usually placed in reserved spaces in the IP header (most proposed solutions use the Identification field). The overhead associated with this method are mostly in terms of the packet space and modification required in the IP header, as well as the router processing time required.

Various schemes differ in the type of markings they use, as well as in the points where a node is required to mark. For example in [10], the marking code is a half of the IP address octets (i.e. 16 bits) plus one extra bit to indicate which half and a 17 bit storage on the packet, comprised of the 16-bit ID field and the 1-bit reserved Flag bit is used to hold this information, while in [21] an encoding scheme based on router-level topology is proposed to be stored in a futuristic IPv6 packet header that makes provision for 52-bits for traceback purposes. We further discuss specific deterministic packet marking schemes in chapter 5.

Probabilistic Packet Marking

Probabilistic schemes counter the space constraint in deterministic packet marking by requiring that a packet is marked with only a part rather than the whole of the path it traverses. Such schemes make the reasonable but not foolproof assumption that attacks are usually made up of a large number of packets, and so by aggregating these partial path information from a number of packets, traceback can be achieved along with path reconstruction. Examples of schemes included in this category are [12, 13, 14, 15, 17].
2.2 Motivation

Our motivation in this research is based on a focus to find a more cost effective approach in deterministic packet marking schemes. Like Al Duwairi and Daniels [21], we propose that a knowledge of Internet maps can be used to advance IP traceback, however our focus is to explore ways to use a knowledge of the autonomous systems nature of Internet as presented in recent Internet mapping projects such as [48, 49, 50, 51], to influence a reduction in the costs of deterministic packet marking and further propose a novel IP Traceback scheme based on our findings.

Our ultimate goal is geared towards a scheme that possesses backward compatibility with existing protocols. We assume that we can that we can employ 25 bits in the current IPv4 header for traceback purposes – a recommendation put forward in [10]. This is comprised of the 17 bits which most traceback schemes already propose for use (i.e. a 16-bit ID field and a reserved bit from the flag field), as well as the 8-bit TOS field, which has been proven to be rarely used and even when used makes no measurable difference in packet delivery.

We are also motivated to provide a scheme that is relatively easier to implement and possesses low processing and zero bandwidth overheads. More importantly, we believe that with the increasing sophistication of Internet attacks, a traceback scheme that needs few parameters in order to achieve traceback objectives is vital and imperative; and so require a solution capable of tracing a single attack packet without widespread deployment, i.e. all nodes that a packet traverses need not be involved in the traceback process. Finally, we also seek a scheme that is capable of a reasonable measure of success at various levels of deployment.
By bringing traceback and network topology research together, and incorporating the more recent advances in Internet mapping, we can create an approach that takes a different view of network topology from an IPT standpoint.
CHAPTER 3. PRESENTATION AND ANALYSIS OF INTERNET MAPS

In this chapter, we briefly discuss past and ongoing work in the area of Internet topology maps, and proceed to present the specific data we used in our work and then present our statistical analysis of the data with an emphasis on results relevant to deterministic packet marking (DPM) schemes.

3.1 Internet Topology Maps

There are many reasons why an understanding of the topology of the Internet is important. Network operators, designers and researchers among other groups of users and operators constantly have needs to collect, analyze and visualize data on connectivity and performance across the Internet. Although the need may be simple and clear enough, such a task on the other hand is by no means trivial. And this is better appreciated when one considers the Internet as an ecosystem [41] that is made of ever-increasing, morphing and very diverse links between even more diverse entities. It is quite interesting if not phenomenal, that an ARPANET project that started out in 1969 with one node in September and four by December [60] has now become an overwhelmingly vast connection of hundreds of millions of hosts interacting through a great number of links. In their book, “Where Wizards Stay Up Late: The Origins of the Internet”, Hafner and Lyon [61] capture what is arguably the most complete information on the conception and birth of the Internet. Notably however, the book neglects many of the changes that occurred in the early nineties, a period that is widely regarded as very definitive in terms of the massive explosion of the Internet and probably the most causative period in what we view today as the cyber ecosystem.
More recently, there have been a few projects dedicated to unraveling the complexity of the Internet and some of the early works in the field include [37] and [41] which began at about the same period in 1998 and have been involved in efforts aimed at providing useful data to assist in mapping the Internet as well as developing and deploying tools towards this end. For example, the Internet Mapping Project [37] which started at Bell Labs in the summer of 1998, led by Burch and Cheswick, began with a goal to acquire and save Internet topological data over a long period of time and make this available in the whole study of routing problems and changes, distributed denial of service attacks (DDoS), and graph theory; and to date the project like similar others has been successful in accomplishing this, and not just for the initial purposes alone but indeed to assist many other research efforts.

Before these, the best available metrics for such ventures were the incidental data that could be garnered from sources such as BGP tables that allow us to have some idea of the connectivity of entities on the Internet as well as perform modest analysis based on these. However, apart from the required cooperation among major players at the so called core of the Internet, such data also lacked the depth required for many research works. For example, University of Oregon Route View Project [50] and RIPE’s RIS (Routing Information Service) [51] are two projects that provide access to BGP tables from several organizations’ routers in addition to furnishing daily statistical analyses from which one can infer AS adjacency. But while it is possible to establish a connection between a pair of ASes from either of these, neither is able to give more detailed information such as a reasonably accurate number of links between a given AS pair. In this work however, and for the purpose of peer validity, we do make comparative analyses between some of the results we derived from our
data and similar metrics obtained from measurements provided by RIPE’s RIS which uses a relatively passive data collection method.

Internet mapping projects typically involve taking a more active approach as well as including specific techniques that are aimed at capturing data that give the best view of the Internet or certain parts of it during the period of collection. The emphasis desired by each project usually determines how well suited it is for specific research purposes, for example, the Cyber-Geography Research project [62] focuses on the more quantitative aspects of measuring and mapping the physical location of entities in cyberspace, whereas the CAIDA Project [49] places more emphasis on an understanding of connectivity and routing. Using an active approach, most Internet mapping projects send out packets of data from one or more sources to many destinations through the Internet in a manner that allows information to be sent back to the source from nodes traversed by the packets. The information gained about the paths that these packets take can then be used collectively and manipulated in various ways to reveal useful metrics that can be employed in determining such indices as physical network connectivity, routing, and performance among other things. As we mentioned before, the Internet is an ever morphing entity and most of the data gathered to reveal its structure can only represent as closely as possible and at best what it is at the time of gathering and for as long as it does not change significantly thereafter – a vital fact that most works, including ours, take into account.

For the purpose of our work, we employed data gathered from two separate projects – CAIDA and Rocketfuel – both of which used active as well as passive methods of data gathering. Subsequent statistical analyses are based on both sets of data.
One of the most common active methods used in Internet mapping projects is traceroutes. Traceroute is a utility that returns as accurately as possible, a path listing of the routers and/or hosts that a packet is traveling through until it reaches its destination. It is pertinent to note that some incongruities have been observed in similar Internet topology measurements obtained from traceroutes compared to those derived from BGP tables. The reasons for these incongruities vary, though possible factors include the difference in approach to measurements as well as the fact that both are based on best possible approximations rather than scientifically accurate mappings. In [65], Hyun et al, proffer a reason for such incongruity in AS path measurements, attributing this to the visibility of exchange points in traceroute paths. As we mentioned before though, the reasons vary and more research work is required in this area. We note however, that more often than not, traceroute measurements present higher values for similar topology measurements, and for our purposes this typically represents worst case scenarios.

3.1.1 CAIDA Data

The Cooperative Association for Internet Data Analysis (CAIDA) is a collaborative undertaking among organizations from the commercial, government and research sectors, with the ultimate goal of serving as a facilitator in addressing engineering concerns relating to topic areas that include macro-level and cross-ISP measurements and analyses, technology evolvement to scale up the performance of the Internet among other similar areas of focus. As part of its operations, CAIDA collects several different data types at geographically and topologically diverse locations using active, passive, and real-time data collection methods, and makes this data available to the research community. The effort also includes the
provision of other incidental but useful data files, for example an IP address to AS mapping file, as well as other tools and scripts.

In a collaboration that started in July 1998 with the Defense Advanced Research Project Agency (DARPA), CAIDA launched a Next Generation Initiative (NGI) – an effort which focuses on monitoring, depicting, and predicting traffic behavior over production and experimental networks. Two components of the project are the development of tools to automate the discovery and visualization of Internet topology and peering relationships through application of CAIDA’s Skitter tool and the provision of storage and analysis of massive volumes of traffic data. It is from these sources that we collected the data used in our research.

Specifically, we made use of the data set referred to by CAIDA as the ITDK (Internet Topology Data Kit) #0304, which consists of CAIDA’s global ICMP traceroute (Skitter) measurements, related IP tables, IP and AS link graphs, parsing scripts, and command sequences, as gathered during a collection interval of April 21 and May 8, 2003. The data includes over 1,134,633 IP addresses and 2,821,559 IP pair links. Among the resources provided are several files containing traceroute data obtained from about 23 monitors (Appendix A provides a list that shows the location and current status of these monitors) in a spatially and topologically diverse set of locations in Asia, Europe, and North America. Figure 2 shows three sample lines from one of these files.
The initial letters “C” and “I” in the first two lines shown, represent complete and incomplete traceroutes respectively. An incomplete traceroute is interpreted as one which for one reason or the other does not furnish the IP addresses of all nodes along the path of packet from source to destination. A third but rare option is a traceroute which is not only incomplete but there is no concrete information on the number of hops missed and where, and this is typically represented with an “N” at the start of the line. The next segments on each line provide the following information respectively: the source address, the destination address, a timestamp, the round trip time, the hop count, and from thereon the known IP addresses of intermediate hosts. Notice the zero values typically recorded for the round trip time and hop count segments of the line starting with an “N” in fig. 2. In section 3.5, we present the analyses we derived from the various measurements available in CAIDA’s ITDK0304.
3.1.2 Rocketfuel Data

The Rocketfuel project like the CAIDA project also uses active methods to probe the Internet for topological information, but unlike CAIDA, their goal was to gain an understanding of ISP topologies as opposed to the wider Internet. For reasons that most likely include security, most ISPs do not readily release their confidential network topologies. At best and where needed many will only publish simplified topologies which lack router-level connectivity and POP structure, and which are usually out of date. The Rocketfuel project was created to assist the research community in gaining access to these types of realistic Internet topologies by presenting new measurement techniques to infer quality ISP maps while using as few measurements as possible. As such Rocketfuel is aptly referred to as an ISP topology mapping engine.

By using BGP routing information to focus efforts on an ISP at a time, and then using ISP specific router naming conventions to understand the topology, and also using an innovative alias resolution technique to find which IP addresses represent interfaces on the same router, Rocketfuel successfully mapped out 10 diverse ISPs [Appendix B]. Unlike CAIDA which used dedicated servers, the Rocketfuel project used publicly available traceroute servers as measurement points. With traceroutes sourced from over 800 vantage points hosted by about 300 traceroute servers, the project mapped 10 ISPs in Europe, Australia and the United States. In the process, a database of over 50,000 IP addresses representing 45,000 routers in 537 POPs and connected by 80,000 links was constructed. As part of their validation efforts, they showed the relevant parts of the maps to three of the ISPs and state that each one confirmed that the maps do reflect their network to a large degree. However, for reasons of confidentiality, there is no mention of the particular ISPs involved in this partial validation –
a point worth noting to the extent that a smaller ISP may be easier to map accurately than a much larger one.

We also noticed a few wide divergences in similar measurements for the ISPs that show up in both the CAIDA and Rocketfuel data. We were able to compare these because both projects associate a globally unique identification, i.e. AS number, to each autonomous network. While we consider that some of these divergences certainly occur due to the difference in collection periods (Rocketfuel data was gathered in December 2002), we hold that the focus and thus method used by both groups plays a more significant part in this. As a result of this and to maintain the individual accuracy of each data set, we were careful not to use both sets of data interchangeably but only as far as drawing inferences for our purposes.

3.2 Definitions

In this section, we provide a definition of some key terms used severally in our analyses:

- **Autonomous System (AS)** – A group of networks under the authority of a single administrative authority.

- **Point of Presence (POP)** – Typically refers to the various physical network locations that make up an AS. May also be described more generally as a logical division of an AS based on parameters set out by the administrative authority.

- **Internet Services Provider (ISP)** – A company that provides Internet connectivity and other related services to usually smaller entities. Note that each ISP may also an AS.

- **Access Router** – Any router within an AS that has any of its link connecting that AS to other ASes.
• **Internal Router** – Any router within an AS that has all its interfaces connected only to other entities within the AS.

• **Node Degree** – The node degree is a measure of the number of outgoing edges from a node to other nodes, which are typically called adjacent nodes. Note that in the case of an AS, the node degree will refer to outgoing edges from any of its access routers to other ASes and does include any number of links between the AS and each pair AS; a similar reasoning also applies in the case of POP node degree.

• **Path Length** – We define the path length as the number of hops traversed by a packet as it moves from source to destination. Depending on the network level view we are considering, each hop may be a router, a POP, or an AS.

• **Undirected Link** – Any link between a pair of IP addresses irrespective of the traffic flow that produced the link. This is distinct from a directed link whereby if a packet hops from node A to node B, a unique link is created and separate from when a packet hops from B to A. (Please note that our analyses and results are based solely on undirected links.)

• **Transit AS** – An AS that is usually an ISP or backbone provider and which typically has a high number of links to other ASes and facilitates the flow of traffic.

• **Origin AS** – An AS that primarily operates as an end-user on the Internet and one which traffic typically flows from and to rather than through.

### 3.3 Statistical Analysis of CAIDA Data

In this section, we present the various statistical analyses obtained from the CAIDA data (ITDK0304), but first we show a summary below. As we indicated earlier, our main focus is
to derive various metrics at specific router-aggregation levels of the Internet, i.e. AS-level and POP-level; however, we also include some router-level indices for the purpose of comparisons:

- Total number of ASes: 12,577
- Average router-level node degree: 6.34 (obtained from CAIDA analyses)
- Maximum router-level node degree: 1071 (obtained from CAIDA analyses)
- Average router-level path length: 18.31
- Maximum router-level path length: 35
- Average AS-level node degree: 119.99
- Maximum AS-level node degree: 84,710
- Standard deviation of AS-level node degree: 1488.98
- Most frequent AS-level node degree value: 2
- Highest number of connections between an AS pair: 10,415
- Average AS-level path length: 4.13
- Maximum AS-level path length: 10
- Standard deviation of AS-level path length: 0.795

3.3.1 AS Node Degree

One of most important and useful metric in most Internet measurement projects is the level of connectivity between entities, and this is normally evaluated as the node degrees of the various elements within the network. To obtain the node degree from the ITDK0304, we
used the file containing a list of unique and directed IP pair links as obtained from the traceroute data, and ran it through the following processes:

1. Removal of directionality: As far as the node degree is concerned an edge between nodes A and B is simply one edge irrespective of how traffic flows along that edge, thus for any two pairs A-B and B-A in the file, we considered only one case of these and discarded the other.

2. Using the resource file that contains all known IP address to AS mappings, we converted the refined list of IP links to AS links.

3. Next we collated the total AS connectivity for each AS while maintaining pair level connectivity information for the AS, and obtained the individual AS node degrees.

In figures 3 and 4, we present graphs that show the AS node degree frequency and node degree distribution respectively.
As we stated earlier, and as shown in figure 3, the most frequent node degree is 2, with 664 (5.28%) of the 12,577 ASes having that number of external edges. Not quite evident from the graph above are the minimum and maximum node degrees, which are 1 and 84710 respectively, with 314 ASes having the minimum node degree while expectedly only one AS had the very high maximum value. The average node degree was found to be 119.99, and the standard deviation was 1488.98. As is evident from the distribution of node degrees shown in figure 4, approximately 90% of ASes observed had a node degree value of 128 or less.
Figure 4. AS Node Degree Distribution
Based on the suspicion that a few of the high node degrees were largely responsible for the relatively high average AS-level node degree compared to the average router-level node degree (i.e. 6.34), we recalculated and compared similar statistics after excluding 1255 (approximately 10%) of the nodes with the highest degrees, and the result obtained is reported in table 1. Not surprisingly the average drops sharply to 23.84 along with a corresponding drop in the value of the standard deviation to 27.23.

<table>
<thead>
<tr>
<th>Data Set</th>
<th>Average</th>
<th>Min</th>
<th>Max</th>
<th>Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>All 12,577 ASes</td>
<td>119.99</td>
<td>1</td>
<td>84710</td>
<td>1488.98</td>
</tr>
<tr>
<td>Excluding the largest 10%</td>
<td>23.84</td>
<td>1</td>
<td>133</td>
<td>27.23</td>
</tr>
</tbody>
</table>

Table 1. Statistics of AS Node Degree

3.3.2 AS Path Length

The AS path length measures the number of AS nodes that a packet traverses as it goes from source to destination. Since a packet normally hops through one or more router nodes while traversing an AS, the AS path length is always less than or equal to the corresponding router path lengths. To derive measurements for the AS path length, we used the raw traceroute data files provided in the CAIDA resource kit and applied the following processing:

1. Extraction of all complete traceroute paths from each file, i.e. those lines which are flagged “C”, and aggregate these into a single file.
2. Strip off unneeded segments in the resultant file, specifically we remove the ‘C’ flag, timestamp, RTT, and hop count segments.

3. Converted IP addresses to their corresponding AS mapping – for as many IP addresses as have such mappings. Lines containing IP addresses for which there are no distinct AS linkages are removed following this.

4. For each continuous string of the same AS, we represent the string with a single unique AS number. Note that this means if the same AS has strings separated by another AS string, (i.e. as would occur if a packet exits an AS and makes an ingress into another AS before making a reentry into the initial AS), these would count as two separate AS hops. However, efficient routing means such a situation would of course be rare, and we found no such cases.

5. A count of each unique AS hop is done for each line and the result is collated.

For ease of processing and due to the large number of traceroute paths, we used data obtained from a specific CAIDA monitor (which we refer to as Tokyo-1) and after applying the above processes, we were able to consider over 60,000 traceroutes paths. In figures 5 and 6, the frequency of AS path lengths and the corresponding cumulative distribution derived from this data set are shown respectively. The most frequent AS path length derived is 4, while the minimum and maximum are 2 and 7 respectively. (Note that from data sets from other monitors that we looked at and which we discuss later in this section, the highest maximum path length observed was 10.) The average AS path length is approximately 4.13 and we calculated a value of 0.795 for the standard deviation.
Figure 5. AS Path Length Frequency

Figure 6. AS Path Length Distribution
In figure 7 below, we present the individual AS path length distribution for 7 select monitors – 2 each from locations in Europe and Asia, and 3 from locations in North American. It can be observed from the graph that though the location of the monitor does have an effect on the distribution, the essential point is that at over 98% the AS path lengths converge to 7 hops. Table 2 shows the various average path lengths for each of the monitors.

![Graph showing AS path length distribution for select monitor locations](image)

**Figure 7. Comparison of AS Path Length Distribution for Select Monitor Locations**
3.3.3 AS Unique-Neighbor Degree

Another statistic of interest that derives from the AS node degree calculations in section 3.3.1 is the number of unique neighbors that each individual AS has. In this case, we do not take cognizance of the number of links that exists between a given AS and its neighbor but are interested only in the number of outgoing edges to unique neighbors. We found that in terms of this metric, the maximum degree falls to 3,214 – a notable difference compared to a value of 84,710 given earlier for maximum AS node degree; while the minimum unique-neighbor degree expectedly remained 1. Figures 8 and 9 below show the frequency and cumulative distribution for the unique-neighbor degree. The most frequent value remained as 2, but with more ASes (3,936 of the total 12,577 ASes) having this many number of unique neighbors. More interestingly, the average node degree in this case is 6.55, which is practically at par with the average router-level node degree of 6.34. We also found that 12,358 ASes, representing a little over 98% of the total number of ASes, have a unique-neighbor degree of 32 or less.

<table>
<thead>
<tr>
<th></th>
<th>Tokyo-1</th>
<th>Maryland</th>
<th>Tokyo-2</th>
<th>Urbana</th>
<th>London</th>
<th>Marina</th>
<th>Amsterdam</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>4.1320</td>
<td>3.5376</td>
<td>5.2328</td>
<td>4.6914</td>
<td>2.9527</td>
<td>4.8248</td>
<td>3.7893</td>
</tr>
</tbody>
</table>

Table 2. Mean AS Path Length per Monitor
Figure 8. AS Unique-Neighbor Degree Frequency

Figure 9. AS Unique-Neighbor Degree Distribution
3.3.4 Transit AS Statistics

For reasons directly related to the traceback schemes that we propose further on in chapter 4, there was a need to define and observe two sets of statistics obtainable from the raw traceroute data. These are the frequency of highly-connected ASes, which we interpreted to be transit ASes, as well as the count of ASes occurring in a forward before the first highly-connected AS in individual traceroute paths.

Observation of the results given in the AS-level node degree distribution, reveals that approximately 95% of ASes have a node degree that is less than or equal to 256. Based on this, we arbitrarily defined a highly-connected AS (we interchangeably refer to these as transit ASes) as any AS having a node degree value that is over 256. Next, we processed the traceroute data in the same manner as we did to get path length information, but with an emphasis on obtaining the number of occurrences of highly-connected ASes in each traceroute path. Figure 10 shows the frequency of each count, while figure 11 shows the cumulative distribution.

The second measurement is a count of initial origin ASes occurring in a packet’s path before the first highly-connected AS is traversed. Since if we consider the raw data which shows the forward paths of each packet, there is bound to be a bias based on the locations of the monitors, we instead reversed the paths, effectively considering more thousands more origins than the initial 23 that the monitor locations make possible. Quite interestingly, we found that most packets (approximately 98%) either originated from or had a next hop that is a transit AS. The associated graphs for this measurement are shown in figures 12 and 13. And in table 3 the mean, mode, minimum, maximum and standard deviation values for the two AS transit indices discussed here are provided.
Figure 10. Frequency of Number of Transit AS per Path

Figure 11. Cumulative Distribution of Number of Transit AS per Path
Figure 12. Frequency of Number of Initial Origin AS in a Path

Figure 13. Distribution of Number of Initial Origin AS in a Path
### Table 3. Statistical Values for Transit AS Indices

<table>
<thead>
<tr>
<th>Transit AS Index</th>
<th>Mean</th>
<th>Mode</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency in paths</td>
<td>3.515</td>
<td>4</td>
<td>1</td>
<td>7</td>
<td>0.829</td>
</tr>
<tr>
<td>Initial Origin ASes</td>
<td>0.393</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0.537</td>
</tr>
</tbody>
</table>

3.4 Statistical Analysis of Rocketfuel Data

The CAIDA data set gives adequate information on AS-level Internet mapping but it does not include useful data for POP-level measurements. Based on the increased need for this type of data, the organization has indicated that one of its main goals in the near future is deriving a POP-level map of the Internet. To get a view of POP-level mapping however, we use measurements provided from the Rocketfuel project. We restate that we did find a few discrepancies between similar data for the same AS given by Rocketfuel and CAIDA – for example Rocketfuel records the node degree for AS 3356 (Level3) as 13,000 which is widely different from the same metric given by CAIDA, i.e. 84710. Therefore, we only use measurements from the Rocketfuel project to make certain inferences and suggestions in chapter 4.

3.4.1 POP Node Degree

Again for reasons related to traceback schemes proposed in our work, we found the need to devise a method to divide highly-connected ASes to smaller components. The most intuitive
and logical division thus became one that most such ASes already use, i.e. a POP-level division, which as we stated earlier is typically based on location but may also be based on other logical parameters.

Since Rocketfuel provides data about the POP-level structure of 10 specific ISPs as well as other ASes incidental to the process involved in mapping these, in the data set marked “2003” and made available on the Rocketfuel website [48], we were able to extract POP node degree information, from a number of AS-pair files, for a wide range of ASes including highly-connected transit ASes such as Level3, and also origin ASes which typically have a low connectivity.

![Figure 14. POP Node Degree Frequency](image-url)
A typical AS pair file shows the number of connections that exists between two ASes at different POP locations. The results obtained from these are shown in figures 14 and 15. Interestingly, the most frequent POP node degree is 0, indicating that a lot of the POPs observed have no outgoing edges to other ASes. The maximum degree observed is 70.

3.4.2 POP Path Length

The POP path length information was a little harder to derive due to a lack of adequate information of the traceroute files provided by Rocketfuel, where some key data were either
unresolved or not provided. Thus, we obtained an estimate for the average POP path length by sampling traceroutes with enough POP information in those cases where a packet traverses an AS within the Rocketfuel project’s aim. In all we had a sample population of 1000 such cases and discovered that in a little over 95% of cases, the packet traverses three or less POP hops within an AS. Table 4 shows the breakdown for the number of POP hops observed in the sample.

<table>
<thead>
<tr>
<th># of POP Hops</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>178</td>
</tr>
<tr>
<td>2</td>
<td>426</td>
</tr>
<tr>
<td>3</td>
<td>355</td>
</tr>
<tr>
<td>4</td>
<td>33</td>
</tr>
<tr>
<td>5</td>
<td>8</td>
</tr>
</tbody>
</table>

Table 4. Frequency of POP Path Lengths in Sample Data

3.5 Comparisons with RIPE’s RIS Data

As we mentioned earlier in the chapter, an alternative method of gathering a topological view of the Internet is by innovatively using BGP routing information. BGP is an inter-autonomous system routing protocol used to update routing tables and involves a vast exchange of path vector messages in the process. Each message from one router to the next
contains information about a path to some destination network, and the path is usually
defined as an ordered list of ASes that a packet should travel to reach the destination. By
gathering and storing such routing information over a period of time and from different
locations, it becomes possible to make useful topological inferences.
Such a project was started in 1999 as a RIPE NCC project and is called the Routing
Information Service [51]. The project currently has over 300 IPv4 and IPv6 peers at 12 data
collection points in Europe, Japan and North America and these collect and store Border
Gateway Protocol (BGP) routing information and make it publicly available for the Internet
community. The project is ongoing and provides access to both archived and new data. We
have taken care to compare only data taken at about the same periods for both the RIS project
and the CAIDA project; however, there is still an 8 month difference as the available metrics
from RIS was based on data gathered in September 2002.

<table>
<thead>
<tr>
<th>Metric</th>
<th>CAIDA</th>
<th>RIPE RIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean AS Path length</td>
<td>4.13</td>
<td>6</td>
</tr>
<tr>
<td># of ASes Observed</td>
<td>12,577</td>
<td>15,600</td>
</tr>
<tr>
<td>Most frequent AS Path Length</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Maximum Path Length</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>Ratio of Transit to Origin AS</td>
<td>1:10</td>
<td>1:10</td>
</tr>
</tbody>
</table>

Table 5. Comparisons of CAIDA and RIPE RIS Statistics
We stress that we do this only to gain some form of comparative validity for the data we used in our analysis, as any unreasonably wide divergences in similar metrics would be a problem. Table 5 shows the comparison of similar indices from the CAIDA data and the RIS project. We observe that the variation in measurements is indeed very minimal and can most probably be explained by the difference in the methods of data gathering.

Another important piece of information measurable from the RIS project is the rate of change in the number of observed ASes over a period of time. We noticed that while there were 15,600 ASes observed in April 2003, the number for March 2005 had risen to 19,833, i.e. a difference of 4,233 ASes representing an increase of about 27%. While this is likely partly due to an increase in the number of collection points, it is also not unexpected as the Internet remains an ever-growing entity. While we expect such a growth to have a minimal effect on path length, we assume that the effect on node degree may probably be more pronounced further down the line.
CHAPTER 4. PROPOSAL AND EVALUATION OF TRACEBACK SCHEMES

In this chapter, we propose and evaluate different DPM schemes – all informed by our knowledge of the Internet topology results discussed in the previous chapter. We also include a comparison between our schemes and other DPM schemes.

4.1 Underlying Concept to Proposed DPM Schemes

First, we discuss concepts, assumptions, and other information common to the traceback schemes proposed in this work.

As we mentioned in chapter 1, Al-Duwairi and Daniel's work, “Topology Based Packet Marking” explored the possibilities in using topological information to improve the IP traceback, and we apply a similar concept in our work. However different from their work [21], we explore hitherto unconsidered aspects of using Internet topology in a similar manner. Figures 18 and 19 show the primary difference between our approach to IP Traceback compared to other previous works. While most these works have viewed the path a packet takes as composed of several router nodes, we view the same path as being composed of nodes that may each represent a router, POP or AS. While a significant reason to do this is an attempt to discover more efficient marking information encodings, there are other gains that may not be immediately obvious. These include:

- Minimizing router time spent on tracing rather than routing
- Minimizing the storage space required to keep tracking information
- Leveraging the privileges individual classes of ASes possess, e.g. transit ASes can be identified and made central to traceback schemes
Figure 16. Router-level View of a Path on the Internet
4.1.1 Assumptions

The following assumptions are central to the DPM schemes presented further in this chapter:

1. IP Traceback is an infrequent operation compared to routing of traffic.
2. Beyond the routers at the origin AS in an attack, routers further along the path, i.e. routers in intermediate and destination AS are not compromised.
3. That we can utilize 25 bits in the current IP header (as described in section 2.2) for marking purposes.
4. The routing path within an AS is largely constant, i.e. it will rarely change over short periods of time, and such changes are usually eventful enough to be logged.
5. Directly following from the above, we assume that most transit ASes keep good logs of routing events, for instance, changes in static routes.

4.1.2 The Marking and Traceback Processes

As we stated earlier, in the schemes we propose and similar to [21], we view an Internet path as being composed not only of nodes traversed but also the degree of each node; and each node in our schemes may be any of a router, POP, or AS. Referring to figure 19 for example, we note a path with an AS path length of n from the source to the destination. Each AS node along the path has its own node degree, and so a node will mark each packet with information that represents the ingress point of the packet into its network. Since a node with degree d, requires at least \(\lfloor \log_2(d_i) \rfloor\) bits to encode any of its edges, a total of

\[\sum_{i=1}^{n} \lfloor \log_2(d_i) \rfloor\] bits are required to encode an entire path. In addition \(\lfloor \log_2 (\text{max} \sum_{i=1}^{n} \lfloor \log_2(d_i) \rfloor) \rfloor\) will be required for indexing the location where each node will append
its own code. This index is updated by each marking router taking into account that nodes use variable length codes. In our work, we define the maximum summation of nodes along a path as that which we either observe or deduce from paths in our evaluation. To achieve traceback, two methods can be applied. In the first instance, a recent Internet topology map can be used to decode the marking information and each node starting from the destination provides coding which points to the next node, and this process goes on successively until the source is reached. In the absence of such a map however, a traceback query initiated at the victim can progressively query nodes for interpretation of their respective codes until the source is discovered.

4.2 Proposed Schemes and Evaluations

We propose the following three DPM schemes based on topological studies of the Internet:

4.2.1 AS-Level Topology-Based Deterministic Packet Marking

Referring to figure 19, this scheme requires each intermediate AS between the source and destination ASes to place its mark in the packet as the packet traverses through it. The ingress router at each AS is responsible for placing this mark as well as incrementing the index by a value equal to the number of bits required to encode all of the AS’s external edges, i.e. \( \lceil \log_2(d_i) \rceil \). The mark placed is the actual edge number that an AS assigns to all its outgoing edges and this will be unique within each AS but not globally unique. During traceback, the destination AS sends a traceback query to the AS it receives the packet from, which will typically be the egress point of that AS. The traceback-enabled router at the egress
checks the index to know where to begin reading off the AS's mark, and obtains and
interprets this mark to discover the egress point of the pair AS that sent the packet. This
router also decrements the index by its AS's encoding ceiling, i.e. $\lceil \log_2(d_i) \rceil$ and then sends
the query along to the next AS in the packet's reverse path. This process continues from one
AS to the next until the source is discovered. We evaluated the probable number of bits this
scheme will require by running the scheme against the traceroute paths discussed in chapter
3, and present the frequency and distribution of our results in figures 20 and 21.

![Histogram of Number of Bits](image)

Figure 18. Frequency of Sum of Ceiling of Bits Required to Encode Paths
As seen from the figures shown, the maximum number of bits required to encode an entire path is 92, and when we compare this to the value obtained in [21] for a router-level scheme, i.e. 46 bits, it is apparent that this value is twice that. While there is still the advantage of minimizing router time spent on marking, the significant rise in bits makes the scheme futuristic at best. Note that the total number of bits required will thus be 99, when we including the extra bits needed for indexing.

![Figure 19. Distribution of Sum of Ceiling of Bits Required to Encode Paths](image)

We determined in chapter 3 that transit ASes, which typically have very high degrees, make up over 75% of most packet paths, and deduced this to be the reason for the very high results
obtained here. While considering an AS-level view does significantly reduce the path length compared to a router-level view, the transit ASes with high node degrees remove any advantages this would have offered to the resultant number of bits needed for encoding. One solution, we propose to this is to explore ways by which we can reduce the impact of these highly connected ASes in the encoding of the path of a packet. And our first option is to consider the transit ASes on a POP-level. From the results we showed in chapter 3 based on the Rocketfuel data, we propose that this division will yield favorable results since the highest node degree for observed POPs is 43, a very significant reduction from the same value for observed ASes – 84710. Of course this substitution comes at a cost and increases the path length for each transit AS to the number of POPs the packet traverses within the AS, and we found this to be typically within the range of 1 to 3. Inadequate data from the Rocketfuel data however, made it impossible for us to evaluate this modification to the scheme, and we have proposed this as part of our future work.

With respect to path reconstruction, this scheme will at the least reconstruct a partial path (assuming we seek the more common router-level path) of the packet as part of the traceback process itself, with missing router hops being those within individual AS ingress and egress points in a packet’s path. However, and based on our assumptions, there still exists the possibility of achieving a full path reconstruction by taking advantage of the routing that can be obtained from most ASes, such that the path from a given ingress point to an egress point can easily be determined based on the ASes routing tables. This will however, require cooperation from the particular AS in each case.
4.2.2 AS-Level Deterministic Packet Marking using Unique-Neighbor Marks

The second option to reduce the impact of the transit ASes forms the basis of our next scheme where we change the marking information an AS places within a packet from an edge number based on all outgoing edges, to an edge number based only on unique neighbor edges. As we stated in chapter 3, there is a significant reduction (mainly for transit ASes) in node degrees when based on unique-neighbor edges as opposed to all outgoing edges, and this is typified by the maximum in each case, i.e. 3214 and 84710 respectively. We also evaluated this scheme on the available traceroute paths and figures 22 and 23 show the frequency and distribution for the number of bits required for path encoding.

Figure 20. Unique-Neighbor: Frequency of Sum of Ceiling
The reduction in the number of bits needed in this scheme compared to the first is 34 bits. The maximum number of bits required is 58 although over 95% of paths could be encoded with 46 bits, a result that is similar to the DPM scheme proposed in [21]. The not too apparent trade-off in this scheme however, is the ability to provide a full path reconstruction. Traceback is still achieved as before by following the reverse path from one AS to the next, but because each neighbor AS to the marking AS is only marked as one edge irrespective of
the number of edges that may occur between both ASes, neither the egress nor ingress points can be deduced from in this situation, and thus reconstructing a detailed path is hardly feasible.

4.2.3 Globally Unique Marks for Transit AS Class

Our third scheme based is based on the topological measurements for transit ASes discussed in chapter 3. The scheme involves assigning fixed bit sizes to different classes of ASes. As we noted previously, in all the paths observed:

- One or more transit ASes appeared in a given path
- Transit ASes appeared in a string, and we observed no case where a packet traverses from one transit AS to an origin AS and back to another transit AS.
- We observed very rare cases (approximately one in 40,000) in which a packet traverses 3 origin ASes consecutively.
- 97.5% of paths either started from a transit AS or traversed into a transit AS on the next hop from the source.

Based on the above, we propose a scheme in which transit ASes are given a globally unique number, which we refer to as the AS marking number (ASM#). Given that there are approximately 700 transit ASes, it means we require 10 bits to encode any ASM# and propose that 10-bits from the 25 bits available for marking be reserved for this purpose. We also propose that a further 12 bits be reserved for unique-neighbor markings for transit ASes, while the remaining 3 bits will be used for marking by origin ASes along the path (see figure 22). The 12 bits is based on our observation that the highest unique-neighbor degree is 3214.
In this scheme, we require a trust system such that marked packets received from transit ASes have no need to be marked again either by another transit AS or an origin AS.

<table>
<thead>
<tr>
<th># of Origin AS</th>
<th>Neighbor#</th>
<th>ASM#</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 bits</td>
<td>12 bits</td>
<td>10 bits</td>
</tr>
</tbody>
</table>

Figure 22. Fields in the Globally Unique Marks Scheme

The first transit AS that a packet traverses along the path (and this may also be the source AS if the packet’s source is a transit AS), places two marks on the packet – its globally unique ASM# and also its neighbor number to indicate to itself from which AS it is receiving the packet from. From that point forward, and as the packet is passed to successive ASes, it receives no other marks. If at the destination, the packet is found to have caused an attack, the victim reads off the 10 bits reserved for ASM numbers and deduces which transit AS marked the packet, which is also the first transit AS to receive the packet. A traceback query can be sent to this AS with the neighbor number included as part of the query, and the AS is able to interpret its unique neighbor number to determine which AS it received the packet from. In a case where the transit AS is also the source of the packet, then the value of the Neighbor# is either left as all 0’s by the AS to indicate this situation, or a mark conveying some extra information about the source of the packet within the AS can be placed instead. Note that the latter will only be possible in cases where an AS that does not require the entire 12 bits to mark its unique neighbors, otherwise an ambiguity will arise. In the case where a packet either starts off from a transit AS or hops to a transit AS from its source, then
traceback can be conclusively achieved here, and as we stated earlier about 97.5% of paths observed conformed to this case.

In the instances where a packet hops from an origin AS to one or more other origin ASes before hopping into a transit AS, we have created a third marking field of 3 bits. This field is a counter that will be incremented by any origin AS which receives a packet from another origin AS. For example, if a packet hops from an origin AS to another origin AS before traversing a transit AS, the intermediate AS in this scenario increments the counter by 1. This serves a number of purposes. It can convey information to a victim tracing a packet whether or not the information it receives from a transit AS in a query is a final pointer to the source of the packet or if one or more intermediate origin ASes occur along the path. Armed with such extra information and either a recent Internet topology map or cooperation from the intermediate AS, the victim can view ASes connected to this origin AS as possible attack sources. There is a loss of precision in this case, however, we again note that these cases are rare and occurred only in 2.5% of the paths we considered.

In this scheme, there is a higher loss in path reconstruction information, but the apparent gain is the reduction in the number of bits required to achieve traceback makes it possible for use with existing network protocol and infrastructure environment. In addition, the reduction in the number of entities required to achieve traceback as well the possibilities of partial deployment (which we discuss below) make the scheme unique.

4.2.3.1 Partial Deployment of GUM

To test the possibilities of a partial deployment of the GUM scheme, we set up an experiment to randomly choose transit ASes that will deploy GUM at various stages of deployment. For
instance, if we consider the instance of a 10% deployment stage, we randomly select 10% of the transit ASes and assume that these are running GUM; we then observe how far along each traceroute path these selected ASes occur (if at all they do) to mark the packet. We take ten instances of random selections at each deployment stage, repeating the process of observation for each selection, and recording a cumulative percentage for each point on the path that one of the selected transit ASes occurs in the paths. Thus point 0 means that a selected transit AS is the source, while point 1 indicates it is the next hop from the source, and so on. A “no mark” case occurs in a situation in which none of the randomly selected ASes shows up in a path, and thus a packet will not be marked from source to destination. We then repeat the entire process for another stage of deployment, i.e. at 50% deployment (denoted as p=0.5). The results obtained are presented in table 6, and we note that at 50% deployment, only about 3% of packets will not be marked at all. But if we are to consider the ideal case in GUM, which is for a mark to be placed at most two hops from the source, then at 50% deployment, about 65.5% of the packets will be marked at most two hops away from their sources, while at 70% deployment, the percentage increases to over 87% of packets. The corresponding percentages at 90% and 100% deployment stages are 97.5% and 99.98% respectively.
### Security Issues

In this section, we discuss security issues relevant to the schemes we have proposed:

1. The first issue, which is relevant to the first two schemes, is the case in which an attacker attempts to fill up the spaces apportioned for marking. This is countered by the use of both an index and a cyclic storage format, such that once the packet leaves the attacker’s network, other nodes can write over such false marks while using the index to indicate where those marks are placed.

2. The second issue involves the third scheme. An attacker at an origin AS may input fake ASM and neighbor numbers before sending the packet along. However, the protocol requires that any transit AS receiving a packet from an origin AS must input both of these numbers and so the first transit AS simply overwrites any such marks placed by the attacker. We propose that in such a case, a transit AS noticing the field has been marked when it is receiving a packet from an origin AS should generate an ICMP to indicate this anomaly. This ICMP can be sent to the administrators of the transit AS, the destination AS and also the destination AS claimed in the source address field.
3. An attacker may also intelligently input marks into the packet in the case of the first two schemes such that the marks will point to its connected neighbors during the traceback process. Our suggestion to deal with this is to make use of average topological metrics (e.g. path length) during traceback and consider all nodes that fall within the expected source, with the knowledge that the attacker is likely located within the path. Also useful and where available, is the use of other similar packets which may have followed different paths based on routing changes. The closest (that is, from the victim’s perspective) common AS along the packets’ paths will very likely be the attacker’s network.

4. In the third scheme, an attacker sitting in any of the transit ASes can input a misleading ASM and neighbor number, and since a trust system exists between transit ASes and all transit ASes are trusted by origin ASes, such a mark will not be detected or overwritten. While this is a promising method of attack, it does require that the attacker must launch the attack from one of the transit ASes, which based on our parameters are about 700 in number.

4.4 Comparison of GUM to other DPM Schemes

In this section we compare the Globally Unique Marks (GUM) scheme with other deterministic packet marking schemes.

Node append [12], which we mentioned in chapter 2, is a DPM scheme where each router appends its own IP address to each forwarded packet, such that the destination can identify the path followed by a packet by inspecting the list of IP addresses found in its header.

Considering the fact that the average router-hop count on a path is 15, the packet overhead to
this scheme is about 480 bits, and the significant increase in the size of the packet leads to bandwidth wastage and to packet fragmentation. The space needed for marking also means that the scheme is not compatible with the current IPv4 header.

Packet Identifier [34], commonly referred to as Pi is a packet marking scheme in which a path fingerprint is added to each packet at nodes, and enabling a destination node to identify packets traversing the same paths through the Internet on a per packet basis, regardless of the IP address claimed. In this way, if a victim classifies a packet as malicious, it can filter out all subsequent packets with the same type of marking which will happen as the scheme is deterministic. The scheme however, is useful only as a filtering tool in the case of an attack like a DoS attack, and does not achieve traceback.

Deterministic Bit Marking (DBM) [63] is another scheme which is targeted towards isolating and discarding DoS attack traffic. Bit marking is done on all packets and at all the routers along the path, creating a common path signature at the destination for all packets originating from the same location. The process involves the marking field being reset at the source and routers altering one or more bits rather than storing router information as a packet travels along the path. It was observed from Internet topology of ASes that the source networks are quite uniformly distributed over the path signature space, and so using DBM, it is possible to identify the origin of an attack in the resolution of an AS. However, the basic assumption is that the origin network is cooperative and the marking bits of packets will be set to zeros initially. Also the topology of participating routers and their bit marking positions must be known to the routers that want to investigate the source of a packet.

Traceback with Deterministic Packet Marking [10] is a traceback scheme which requires all edge routers to participate in packet marking. The marking will be done deterministically, but
all edge interfaces on all edge routers will place either the first or the last 16 bits of their IP address in every incoming packet in the ID field, and set the reserved flag to indicate which part was placed. The victim of an attack collects marked packets to obtain the full IP address of the ingress router and arranges these with cooperation from the source network to find the source. This effectively means that a single packet attack cannot be decisively traced.

Topology Based Packet Marking [21] which we have referred to often in this work is another DPM scheme that makes use of recent Internet maps in proposing a traceback scheme. Like most other previous works however, it also takes a router-level view of Internet paths and has the limitation that it requires marking at all traversed routers. The scheme is also futuristic as it relies on a modification of the current IPv4 header unlike the Globally Unique Marks scheme we proposed in this work.
CHAPTER 5. CONCLUSIONS AND FUTURE WORK

In this chapter, we will summarize our findings and other key points mentioned. We end the chapter by proffering our suggestions towards future works.

5.1 Conclusions

In this work, we were able to make the following contributions:

- We were able to offer an alternative of view of Internet paths from an IP Traceback point of view such that a path traversed by a packet could be represented as nodes composed of routers, POPs, and/or ASes depending on the immediate objective.
- We were able to present various topological metrics from recent Internet maps and in particular for hitherto not readily available data in the AS and POP levels.
- We were able to extrapolate our findings to aid us in proposing three new DPM schemes and present evaluation results that show the feasibility and possibilities available in each scheme.
- We were able to present a DPM scheme that is compatible with the current IPv4 protocol and also capable of successfully tracing a single attack packet on the Internet.
- We were able to show the possibilities and the measure of success expected of our scheme at different stages of deployment.

5.2 Future Work

We make the following suggestions toward future work:
• Evaluation of the modification we suggested to the AS-level Topology-Based DPM scheme with the availability of more adequate POP-level data (from CAIDA or other sources).

• Based on the changing nature of the Internet, a re-evaluation of the Internet topology metrics we discussed in our work and a study of how those changes affect proposed schemes.

• Extrapolation of the statistical measurements of the Internet to assist in improving traceback schemes in other IPT categories different from packet marking.
APPENDIX A. LOCATION AND CURRENT STATUS OF CAIDA MONITORS

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Organization</th>
<th>Location</th>
<th>Status (as at 04/20/05)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a-root</td>
<td>Verisign</td>
<td>Herndon, VA, US</td>
<td>active</td>
</tr>
<tr>
<td>apan-jp</td>
<td>APAN</td>
<td>Tokyo, Kanto, JP</td>
<td>active</td>
</tr>
<tr>
<td>arin</td>
<td>ARIN</td>
<td>Bethesda, MD, US</td>
<td>active</td>
</tr>
<tr>
<td>b-root</td>
<td>ISI</td>
<td>Marina del Rey, CA, US</td>
<td>active</td>
</tr>
<tr>
<td>cdg-rssac</td>
<td>GIP Renater</td>
<td>Paris, France</td>
<td>active</td>
</tr>
<tr>
<td>champagne</td>
<td>University of Illinois at Urbana-Champaign</td>
<td>Urbana, IL, US</td>
<td>active</td>
</tr>
<tr>
<td>d-root</td>
<td>University of Maryland</td>
<td>College Park, MD, US</td>
<td>active</td>
</tr>
<tr>
<td>e-root</td>
<td>NASA</td>
<td>Moffett Field, CA, US</td>
<td>active</td>
</tr>
<tr>
<td>f-root</td>
<td>VIX</td>
<td>Palo Alto, CA, US</td>
<td>active</td>
</tr>
<tr>
<td>h-root</td>
<td>US Army Research Lab</td>
<td>Aberdeen, MD, US</td>
<td>active</td>
</tr>
<tr>
<td>i-root</td>
<td>Autonomica</td>
<td>Stockholm, Sweden</td>
<td>active</td>
</tr>
<tr>
<td>iad</td>
<td>MFN</td>
<td>Washington, DC, US</td>
<td>active</td>
</tr>
<tr>
<td>ihug</td>
<td>IHUG</td>
<td>Auckland, New Zealand</td>
<td>active</td>
</tr>
<tr>
<td>k-peer</td>
<td>RIPE</td>
<td>Amsterdam, North Holland, NL</td>
<td>active</td>
</tr>
<tr>
<td>k-root</td>
<td>RIPE</td>
<td>London, UK</td>
<td>active</td>
</tr>
<tr>
<td>lhr</td>
<td>MFN</td>
<td>London, UK</td>
<td>active</td>
</tr>
<tr>
<td>m-root</td>
<td>Wide</td>
<td>Tokyo, Kanto, Japan</td>
<td>active</td>
</tr>
<tr>
<td>mwest</td>
<td>Worldcom</td>
<td>San Jose, CA, US</td>
<td>active</td>
</tr>
<tr>
<td>nrt</td>
<td>AboveNet Japan</td>
<td>Tokyo, Kanto, JP</td>
<td>active</td>
</tr>
<tr>
<td>riesling</td>
<td>CAIDA</td>
<td>San Diego, CA, US</td>
<td>active</td>
</tr>
<tr>
<td>sjc</td>
<td>MFN</td>
<td>San Jose, CA, US</td>
<td>active</td>
</tr>
<tr>
<td>uoregon</td>
<td>University of Oregon</td>
<td>Eugene, OR, USA</td>
<td>active</td>
</tr>
<tr>
<td>yto</td>
<td>CANET</td>
<td>Ottawa, CA</td>
<td>active</td>
</tr>
</tbody>
</table>
## APPENDIX B. LIST OF ISP'S MAPPED BY ROCKETFUEL

<table>
<thead>
<tr>
<th>AS</th>
<th>Name (Location)</th>
<th>ISP Routers</th>
<th>ISP Links</th>
<th>With Customer &amp; Peer Routers</th>
<th>With Customer &amp; Peer Links</th>
<th>POPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1221</td>
<td>Telestra (Australia)</td>
<td>355</td>
<td>700</td>
<td>2796</td>
<td>3000</td>
<td>61</td>
</tr>
<tr>
<td>1239</td>
<td>Sprintlink (US)</td>
<td>547</td>
<td>1600</td>
<td>8355</td>
<td>9500</td>
<td>43</td>
</tr>
<tr>
<td>1755</td>
<td>Ebone (Europe)</td>
<td>163</td>
<td>300</td>
<td>596</td>
<td>500</td>
<td>25</td>
</tr>
<tr>
<td>2914</td>
<td>Verio (US)</td>
<td>1018</td>
<td>2300</td>
<td>7336</td>
<td>6800</td>
<td>121</td>
</tr>
<tr>
<td>3257</td>
<td>Tiscali (Europe)</td>
<td>276</td>
<td>400</td>
<td>865</td>
<td>700</td>
<td>50</td>
</tr>
<tr>
<td>3356</td>
<td>Level3 (US)</td>
<td>624</td>
<td>5300</td>
<td>3446</td>
<td>6700</td>
<td>52</td>
</tr>
<tr>
<td>3967</td>
<td>Exodus (US)</td>
<td>338</td>
<td>800</td>
<td>900</td>
<td>1100</td>
<td>23</td>
</tr>
<tr>
<td>4755</td>
<td>VSNL (India)</td>
<td>11</td>
<td>12</td>
<td>121</td>
<td>69</td>
<td>10</td>
</tr>
<tr>
<td>6461</td>
<td>AboveNet (US)</td>
<td>367</td>
<td>1000</td>
<td>2259</td>
<td>1400</td>
<td>21</td>
</tr>
<tr>
<td>7018</td>
<td>AT&amp;T (US)</td>
<td>733</td>
<td>2300</td>
<td>10214</td>
<td>12500</td>
<td>108</td>
</tr>
</tbody>
</table>
REFERENCES


[48] Rocketfuel maps and data. 20 Apr. 2005
<http://www.cs.washington.edu/research/networking/rocketfuel>

[50] University of Oregon Route View Project. 20 Apr. 2005
   <http://www.routeviews.org>


<www.securitystats.com/reports/Riptech-Internet_
Security_Threat_Report_vII.20020708.pdf>