

Fall 2014

# Topology dependence of PPM-based Internet Protocol traceback schemes

Ankunda R. Kiremire  
*Louisiana Tech University*

Follow this and additional works at: <https://digitalcommons.latech.edu/dissertations>



Part of the [Other Computer Sciences Commons](#)

---

## Recommended Citation

Kiremire, Ankunda R., "" (2014). *Dissertation*. 221.  
<https://digitalcommons.latech.edu/dissertations/221>

This Dissertation is brought to you for free and open access by the Graduate School at Louisiana Tech Digital Commons. It has been accepted for inclusion in Doctoral Dissertations by an authorized administrator of Louisiana Tech Digital Commons. For more information, please contact [digitalcommons@latech.edu](mailto:digitalcommons@latech.edu).

**TOPOLOGY DEPENDENCE OF PPM-BASED  
INTERNET PROTOCOL TRACEBACK SCHEMES**

by

Ankunda R. Kiremire, B.Sc., M.S., M.S.

A Dissertation Presented in Partial Fulfillment  
of the Requirements for the Degree  
Doctor of Philosophy

**COLLEGE OF ENGINEERING AND SCIENCE  
LOUISIANA TECH UNIVERSITY**

November 2014

UMI Number: 3662481

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.

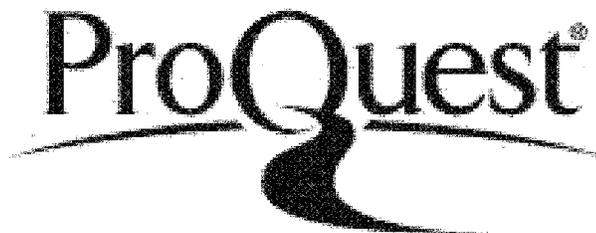


UMI 3662481

Published by ProQuest LLC 2015. Copyright in the Dissertation held by the Author.

Microform Edition © ProQuest LLC.

All rights reserved. This work is protected against unauthorized copying under Title 17, United States Code.



ProQuest LLC  
789 East Eisenhower Parkway  
P.O. Box 1346  
Ann Arbor, MI 48106-1346

LOUISIANA TECH UNIVERSITY

THE GRADUATE SCHOOL

June 20th, 2014

Date

We hereby recommend that the dissertation prepared under our supervision  
by Ankunda R. Kiremire

entitled Topology Dependence of PPM-Based Internet Protocol Traceback Schemes

be accepted in partial fulfillment of the requirements for the Degree of  
Doctor of Philosophy

Vinayakumar S. P. S.

Supervisor of Dissertation Research

Wigley D. D.

Head of Department

CAM

Department

Recommendation concurred in:

Wigley D. D.

Thomas A. B.

Matthew Brust

Justin Kanro

Advisory Committee

Approved:

Jim Palca  
Director of Graduate Studies

Approved:

Sheryl S. Shoemaker  
Dean of the Graduate School

Neil Nagel  
Dean of the College

## ABSTRACT

Multiple schemes that utilize *probabilistic packet marking* (PPM) have been proposed to deal with *Distributed Denial of Service* (DDoS) attacks by reconstructing their attack graphs and identifying the attack sources.

In the first part of this dissertation, we present our contribution to the family of PPM-based schemes for Internet Protocol (IP) traceback. Our proposed approach, Prediction-Based Scheme (PBS), consists of marking and traceback algorithms that reduce scheme convergence times by dealing with the problems of data loss and incomplete attack graphs exhibited by previous PPM-based schemes.

Compared to previous PPM-based schemes, the PBS marking algorithm ensures that traceback is possible with about 54% as many total network packets, while the traceback algorithm takes about 33% as many marked packets for complete attack path construction.

In the second part of this dissertation, we tackle the problem of scheme evaluation and comparison across discrepant network topologies. Previous research in this area has overlooked the influence of network topology on scheme performance and often utilized disparate and simplistic network abstractions to evaluate and compare these schemes.

Our approach to this problem involves the evaluation of selected PPM-based schemes across a set of 60 *Internet-like topologies* and the adaptation of the *network*

*motif* approach to provide a common ground for comparing the schemes' performances in different network topologies. This approach allows us to determine the level of structural similarity between network topologies and consequently enables the comparison of scheme performance even when the schemes are implemented on different topologies.

Furthermore, we identify three network-dependent factors that affect different PPM-based schemes uniquely causing a variation in, and discrepancy between, scheme performance from one network to another.

Results indicate that scheme performance is dependent on the network upon which it is implemented, i.e. the value of the PPM-based schemes' convergence times and their rankings vary depending on the underlying network topology. We show how the identified network factors contribute, individually and collectively, to the scheme performance in large-scale networks. Additionally, we identify five superfamilies from the 60 considered networks and find that networks within a superfamily also exhibit similar PPM-based scheme performance. To complement our results, we present an analytical model showing a link between scheme performance in any superfamily, and the motifs exhibited by the networks in that superfamily.

Our work highlights a need for multiple network evaluation of network protocols. To this end, we demonstrate a method of identifying structurally similar network topologies among which protocol performance is potentially comparable. Our work also presents an effective way of comparing general network protocol performance in which the protocol is evaluated on specific representative networks instead of an entire set of networks.

## APPROVAL FOR SCHOLARLY DISSEMINATION

The author grants to the Prescott Memorial Library of Louisiana Tech University the right to reproduce, by appropriate methods, upon request, any or all portions of this Thesis. It is understood that "proper request" consists of the agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without written approval of the author of this Thesis. Further, any portions of the Thesis used in books, papers, and other works must be appropriately referenced to this Thesis.

Finally, the author of this Thesis reserves the right to publish freely, in the literature, at any time, any or all portions of this Thesis.

Author 

Date 22<sup>nd</sup> October 2014

## DEDICATION

To Abaasa and Ashabe for inspiring, challenging, supporting, and always loving me.

## TABLE OF CONTENTS

ABSTRACT .....	iii
DEDICATION .....	vi
LIST OF TABLES.....	x
LIST OF FIGURES.....	xii
ACKNOWLEDGMENTS .....	xv
CHAPTER 1 INTRODUCTION.....	1
1.1 A Novel PPM-Based Scheme .....	2
1.2 Network Dependence of PPM-Based Schemes .....	4
1.3 Dissertation Contributions.....	6
1.4 Definitions and Terminology .....	8
1.5 Organization of the Dissertation.....	11
CHAPTER 2 BACKGROUND AND RELATED WORK .....	12
2.1 A Background on PPM-Based Schemes.....	12
2.2 Underlying Topologies and PPM-Based Schemes .....	18
2.2.1 A Comparison of Previous Underlying Topologies .....	18
2.2.2 Selecting Representative Marking Schemes .....	24
2.3 Using Subgraphs to Differentiate Networks .....	26
CHAPTER 3 PREDICTION-BASED SCHEME .....	28
3.1 Problem Statement and System Model.....	28

3.2	Our Approach: Prediction-Based Scheme.....	33
3.2.1	PBS: Router Marking Algorithm.....	33
3.2.2	PBS: The Traceback Algorithm.....	36
3.3	Simulation and Results .....	40
3.3.1	Simulation Study .....	40
3.3.2	Marking Scheme Results.....	42
3.3.3	Traceback Scheme Results.....	45
3.4	Conclusions .....	47
CHAPTER 4 NETWORK DEPENDENCY OF PPM-BASED SCHEMES .....		49
4.1	Problem Statement .....	49
4.2	Approach.....	52
4.2.1	Average Path Length.....	53
4.2.2	Overlapping of Attack Paths.....	54
4.2.3	Occurrence of Motifs in Attack Graphs.....	56
4.3	Network Classification Using Motifs and Subgraphs.....	58
4.3.1	Motifs and SRPs.....	58
4.3.2	Identifying Network Superfamilies.....	60
CHAPTER 5 SYSTEM MODEL AND ANALYSIS.....		61
5.1	Traditional Analytical Model.....	62
5.2	The Effect of Motifs on the Analytical Model .....	64
5.3	The Effect of Path Merging on the Analytical Model.....	66
CHAPTER 6 SIMULATION STUDY .....		72
CHAPTER 7 RESULTS AND DISCUSSION .....		77

7.1	Average Path Length .....	77
7.2	Overlapping of Attack Paths.....	78
7.3	Occurrence of Motifs in Attack Graphs .....	80
7.4	Motifs and SRPs .....	84
7.5	Overall IP Traceback Performance.....	88
7.6	Caida Networks.....	92
CHAPTER 8 CONCLUSIONS AND FUTURE WORK.....		95
8.1	Conclusions .....	95
8.2	Future Work.....	97
BIBLIOGRAPHY .....		98

## LIST OF TABLES

Table 2.1:	A comparison of 10 different PPM-based schemes over their features. These features include <i>convergence time</i> , whether they require prior knowledge of the <i>upstream graph</i> to correctly identify attackers, whether they can be <i>incrementally deployed</i> , and <i>underlying topology</i> . The convergence time expressions presented in the table are for a DoS scenario assuming no prior knowledge of the network topology while the underlying topology shows the network topologies used in the evaluation of the schemes. These topologies include <i>single path, single attacker (SP/SA)</i> , <i>single path, multiple attacker (SP/MA)</i> , and <i>multiple path, multiple attacker (MP/MA)</i> .....	16
Table 3.1:	Distribution of packets, and the number of times they are marked, in different graphs. SP/SA = Single Path, Single Attacker; SP/MA = Single Path, Multiple Attacker; MP/MA = Multiple Path, Multiple Attacker .....	44
Table 3.2:	Average number of total packets required for traceback in different graphs .....	44
Table 3.3:	Average number of marked packets required for traceback in different graphs (Traditional traceback / Our traceback scheme).....	45
Table 5.1:	The table shows 4-node subgraphs and the probabilities of the <i>least likely edge</i> for the different marking schemes for $n$ merging attack streams, along side the original probability of the <i>least likely edge</i> given no subgraphs or convergence. The marking probability is denoted by $p$ , the path length by $l$ , the probability of taking alternative routes denoted by $a, b, c$ , with the expressions for PPM, TMS, and PBS shown. For simplicity, it is assumed the probability of taking alternative routes is equal. The convergence time of the marking scheme is indirectly proportional to the lowest probability ..	70
Table 6.1:	Topologies considered, their underlying model, setup settings, average <i>shortest path length</i> (SPL) in hops, the <i>network motifs</i> (M-ID) identified in those networks, and their assigned <i>superfamilies</i> (SF) ...	73

Table 7.1: The average convergence times, measured in packets, for the three Caida networks as well as their 95% confidence intervals after 100 simulations.....	94
------------------------------------------------------------------------------------------------------------------------------------------------------------------	----

## LIST OF FIGURES

Figure 2.1: Internet topology can be captured by a variety of models which include spatial, structural and degree-based models. Each model emphasizes different properties of the Internet and can be used to evaluate network protocols when employed in the Internet. The nodes in these topologies represent devices operating at the Internet layer of the TCP/IP model or the network layer of the OSI model (e.g. routers, switches, hosts). Two nodes are connected by an edge if Internet traffic can be directly transmitted between them without being forwarded by any intermediate nodes.....	23
Figure 3.1: <i>Single Path, Single Attacker (SP/SA)</i> .....	29
Figure 3.2: Prediction-Based Scheme: The marking algorithm.....	35
Figure 3.3: Prediction-Based Scheme: The traceback algorithm.....	38
Figure 3.4: <i>Single Path, Multiple Attacker (SP/MA)</i> .....	39
Figure 3.5: <i>Multiple Path, Multiple Attacker (MP/MA)</i> .....	41
Figure 3.6: Number of marked packets versus distance of last mark for different models. This figure shows how the frequency of router markings in packets received by the victim is dependent on the distance of the router from the victim .....	43
Figure 3.7: Effect of increasing number of legitimate sources on the number of marked packets required for traceback of one attacker (PPM1, Tabu1, PBS1) and two attackers (PPM2, Tabu2, PBS2) .....	47
Figure 4.1: Sample attack graphs from networks built using the described network models. The attack graphs consist of 50 attackers and the paths that the traffic they generate takes to get to the victim node (marked in red). Given that the overall topologies are of the same size, these figures show significant differences in the general structure of attack graphs, which in turn depends on the underlying model used to construct the network topologies.....	51

- Figure 4.2: 2-attacker V-shaped attack graph with different path lengths. Attacker  $A_1$  is two hops away from the victim  $V$  while attacker  $A_2$  is six hops away from the victim. Different attack path lengths have a considerable effect on the convergence time of the attack graph ..... 54
- Figure 4.3: 2-attacker Y-shaped attack graph with overlapping attack paths. Attackers  $A_1$  and  $A_2$  are both six hops from the victim  $V$ , but the attack paths share an overlapping section of two hops. The amount of overlap between different attack paths has a big effect on the convergence time of the attack graph ..... 55
- Figure 4.4: All six possible 4-node undirected subgraphs and their IDs. Only subgraphs 3, 4, 5, and 6 exhibit alternative routes between their member nodes ..... 57
- Figure 4.5: Q-shaped attack graph containing a possible network motif. The traffic from attacker  $A_1$  can take two possible paths on its way to the victim  $V$ . We investigate the influence of motifs in an attack graph by varying the distance of attacker  $A_1$  from the victim, as well as varying the number of attackers by considering multiple attackers  $A_2$ , and  $A_3$ . Motifs in attack graphs influence the convergence times of different marking schemes uniquely, and their level of influence also varies with the number of attackers in the graph ..... 57
- Figure 5.1: Sample attack paths linking attacker A to victim I. The attack path in Figure b exhibits Subgraph 4 in which the traffic can either take path FGI with probability  $a$ , or path FHI with probability  $1 - a$  ..... 62
- Figure 7.1: Convergence times for five V-shaped 2-attacker graphs of equal average length, with 95% confidence intervals. This plot shows that even with identical values for average path length, the distance of the attackers relative to each other affects the considered schemes in different ways ..... 78
- Figure 7.2: Convergence times for 11 Y-shaped 2-attacker graphs of equal average length, with 95% confidence intervals. This plot shows that the convergence time of the considered schemes is affected by the percentage of the attack path that is common to more than one attacker ..... 80

- Figure 7.3: Convergence times for a Q-shaped attack graph under varying conditions, with 95% confidence intervals. Within each plot, the distance of attacker  $A_1$  from the subgraph at victim  $V$  is varied from 1 hop to 25 hops. Between each plot, the number of attackers is increased by one, i.e. Figure (a) just considers traffic from  $A_1$ , Figure (b) considers traffic from  $A_1$  and  $A_2$ , Figure (c) considers  $A_1$ ,  $A_2$ , and  $A_3$ , while Figure (d) considers  $A_1, A_2, A_3$  and  $A_4$ . These plots show that the motif in the attack graph has a distinct influence on the convergence time of different marking schemes and this influence also varies with the number of attackers in the graph.. 82
- Figure 7.4: Subgraph ratio profiles (SRPs) for all networks as well as the five identified superfamilies..... 85
- Figure 7.5: Correlation map for the network SRPs arranged by similarity. The correlation map shows the levels of similarity between the different network SRPs and is used to give a visual indication of how many groups the networks can be placed into ..... 86
- Figure 7.6: The cluster decision plot which shows intra-cluster error  $e(m)$  and percentage change in error  $\frac{e(m+1)-e(m)}{e(m)}$  versus number of clusters  $m$ . The percentage change in error is used to quantify the benefit of increasing the number of clusters from  $m$  to  $m + 1$ . The cluster decision plot is used to determine an accurate ideal number of clusters from the SRPs of the networks ..... 87
- Figure 7.7: Convergence times for PPM, TMS, and PBS, with their 95% confidence intervals, in 60 different networks arranged according to the superfamily they belong to. The line plots (shown in black and purple) show the expected convergence times for the schemes as evaluated using the traditional analytical models and the networks' average shortest path values (cf. Table 2.2 and Section 5.1). The black line plot shows the expected convergence times for PPM and TMS, while the purple line plot shows PBS' expected convergence time. The plot shows that the convergence time for the different schemes varies from one network to another, and in most networks exceeds the expected convergence time based on analytical models. Furthermore, this plot shows that the best performing scheme in one network is not necessarily the best performing scheme in another network ..... 90
- Figure 7.8: The subgraph ratio profiles (SRPs) of the three Caida networks. These networks are similar to each other and yet different from the SRPs of the five superfamilies..... 93

## ACKNOWLEDGMENTS

This dissertation is the representation of years of work, the completion of which would not have been possible without the support, encouragement, and guidance of many people, only some of whom are mentioned here. Their help and support took many forms at different times, ranging from insights into and guidance through the field of IP traceback, to a home cooked meal, or a cup of coffee with some encouraging words. I am very aware that I could not have started and completed the marathon that was this PhD without every single one of these people.

I am grateful to my PhD advisor, Prof. Vir V. Phoha, for convincing me to pursue this program and guiding me along the way. Prof. Phoha was instrumental in helping me identify my research topic, and exposing me to the nitty gritty aspects of research in the fields of computer science and mathematics.

I would like to thank my advisory committee – Dr. Weizhong Dai, Dr. Travis Atkison, Dr. Jinko Kanno, and Dr. Matthias R. Brust – for their advice and guidance towards the completion of my dissertation. I would like to especially thank Dr. Matthias R. Brust for his support. He was instrumental in driving this research and is a co-author in all the papers published from this dissertation.

On the other side of the guidance and support spectrum, I would like to thank my family – my father Bernard Kiremire, my mother Noreda Kiremire, my siblings Grace Ashabe and Abaasa Rwemereza, and the rest of the extended Kiremire,

Gasaatura, and Bwire families. I would not have been able to embark on and complete this journey without the stability, love and encouragement they provide. They always have, and always will be the people I aspire to emulate, the people I hope to make proud, and perhaps inspire to even greater things.

Keeping in line with family, I would like to thank the Casey family – Jessie, Sandy, Jessica, Josh, Jake, and Charlotte. Thank you for taking me in, caring for me, and making the transition from Uganda to Louisiana not just seamless but exciting. I also want to thank the Miller and Corbett families for their hospitality and encouragement.

By far, the biggest group I want to thank is that of my friends, many of whom are unnamed, all of whom were instrumental to my personal and intellectual growth. Thanks for keeping me centered, grounded, and passionate about research and life in general. Special thanks to Alicia D. Boudreaux for proofreading all my writing, listening to my rants, and having the uncanny ability to always *make me smile*. Thanks to my roommate David Irakiza for walking with me through this entire journey, and putting up with all the noise/music I made while at home. Thanks to Krystal Corbett, Jana Melvin, Oneka Cummings, Sara Haler, Jundong Chen, Francois Crochepeyre, Emile Frey, and Carina Shultz. Thanks also go to Sanyu and Brian Kaganzi, Brigitte Kusiima, Gideon Muhiima, Andrew Atuhaire, Joshua Niyo, Joseph Bisoke, Timothy Timbiti, and Joel Muhumuza.

I would like to thank all the people who were members of our research lab at one point or another – Dr. Enam Karim, Dr. Abdul Serwadda, David Irakiza, Jundong Chen, Abena Primo, Zibo Wang, Shafaeat Hossain, Rajesh Kumar, Diksha

Shukla, Saba Ramazani, Drew Gardner, Brenda Stapleton, Rachel Parks, Lexie Dixon, Dr. Abir Rahman, Dr. Justin Rice, Dr. Miguel Gates, and Dr. Kiran Balagani. They were all instrumental in maintaining the supportive and inspiring environment that is the *Center for Secure Cyberspace*.

Above all, I would like to thank Jesus Christ, who through this dissertation has once again proved to me that He is “able to do immeasurably more than all we ask or imagine, according to His power that is at work within us.”

# CHAPTER 1

## INTRODUCTION

*Denial of Service* (DoS) attacks are a form of attack in which legitimate users of a service or resource are intentionally denied access to it by attackers. In the context of networking and computing, DoS attacks typically take the form of a targeted server being flooded with bogus Internet traffic causing overloading and, finally, making it unavailable for its legitimate users [14]. In DoS attacks, the bogus traffic originates from a single source while a *Distributed Denial of Service* (DDoS) attack originates from multiple sources. One popular approach to tackle this problem is *Internet Protocol* (IP) traceback in which the source of the attack is traced and identified using the traffic that constituted the attack.

One technique for realizing IP traceback for flooding style DDoS attacks is *Probabilistic Packet Marking* (PPM) [38], which is the basis for multiple similar schemes, hereafter referred to as PPM-based Schemes. Each PPM-based scheme consists of two processes: a *marking algorithm*, and a *traceback algorithm*. The marking algorithm ensures that network routers embed their own identities in packets randomly selected from all the network traffic that the routers process [38]. In the event of an attack, the victim executes the traceback algorithm which uses the router

identity markings present in the received attack packets to reconstruct the *attack graph* – the paths taken by attack traffic – and establish its sources [39].

### 1.1 A Novel PPM-Based Scheme

Space constraints in network packet headers, where the router identities are typically embedded, leads to a problem of data loss with previous marking schemes. The data loss problem is experienced when routers randomly select packets that already have upstream router information and re-mark those packets in the process. This typically results in the victim receiving fewer packets with upstream router identities than packets with downstream router information. Any limitation in marked packets from any portion of the attack path in turn restricts how quickly the attack graph can be reconstructed and attack sources identified.

Another problem with previous PPM-based schemes is displayed in their reconstruction algorithms. Typical reconstruction algorithms only utilize attack traffic to reconstruct the attack graph. This reliance on attack traffic means that if the victim does not receive any packets with markings from any particular router in the attack path, the algorithm fails to reconstruct a complete and accurate attack graph. This poses a problem particularly with attacks experienced over a short duration.

These problems with the marking and reconstruction algorithms make PPM-based schemes an infeasible approach to IP traceback particularly with DDoS attacks. They typically require the victim to receive a large number of attack packets in order to trace one attacker, which translates to poor time and space complexity [51], and

this problem is magnified when there is a need to trace more than one attacker, as is the case in DDoS attacks [49].

In the first part of this dissertation, we present our contribution to the family of PPM-based schemes: the *prediction-based scheme* (PBS). PBS consists of independent marking and reconstruction algorithms designed to overcome the above mentioned problems. The PBS marking algorithm can be used with other reconstruction algorithms and the PBS reconstruction algorithm can be used with other marking algorithms. Our marking algorithm ensures that the victim receives packets with router identities from all parts of an attack path with equal frequency. To achieve this, our marking algorithm prohibits the re-marking of packets and compensates for any missed marking opportunities. On the other hand, our reconstruction algorithm uses legitimate traffic collected before or after an attack to complement attack traffic in reconstructing the attack graph.

Results show that the PBS marking algorithm only requires about 54% of the *total* packets necessary for traceback to be possible compared to PPM. Additionally, our traceback algorithm extension requires as low as 33% of the usual number of *marked* packets for a complete graph construction in some cases. Dealing with multiple attackers is therefore more practical using PBS than other PPM-based schemes. Furthermore, PBS shows that missing information from routers in the attack path does not, as it previously did, present a dead-end in traceback.

## 1.2 Network Dependence of PPM-Based Schemes

A lot of intensive research has gone into designing PPM-based schemes that are computationally more efficient and robust than the original PPM [9, 38]. However, little work has gone into identifying network dependent factors that affect the performance of PPM-based schemes in large-scale networks. In fact, most simulations are carried out on disparate tree-structured topologies which exhibit a single path from an attacker to the victim. Analytical models derived from these topologies are then used to predict the performance of the schemes when deployed in a large-scale network such as the Internet [49, 30, 52, 44]. However, tree-structured underlying topologies ignore the prevalence of load balancing routers which have the effect of utilizing alternative routes between traffic sources and destinations [2]. This makes it difficult to predict scheme performance in a well-connected large-scale network without implementing the scheme on that network. Additionally, since the schemes are implemented on disparate networks, it is difficult to compare the performance of different schemes directly.

Consequently, there is a need to study the influence of network topology on PPM-based scheme performance. There is also a need to provide some classification criteria for large-scale networks within which scheme performance is possibly comparable, i.e. to be able to predict that two networks would exhibit similar scheme performance without implementing the scheme in both networks. Such a study would reveal the network topology factors that should be considered when designing PPM-based schemes for large scale networks such as the Internet. The study would also enable

researchers to make more informed predictions about scheme performance in large-scale networks without having to implement the scheme in the networks.

In the second part of this dissertation, we present such a study. We identify three network dependent factors that affect scheme performance in large-scale networks. These factors include the average shortest path length, the overlapping of attack paths, and the occurrence of network motifs in attack graphs. Using specific attack graphs, we show the influence of each factor on selected PPM-based schemes. We then use 60 *Internet-like* networks to show how all the identified factors collectively contribute to the performance of PPM-based schemes in more realistic scenarios. The set of networks is selected to encompass a variety of mathematical models used by researchers to create networks that adequately describe the structure of the Internet. We also adapt the *network motif* technique to identify structurally similar groups of networks – referred to as *superfamilies* – from within the set of considered networks [34, 33].

Results show that PPM-based scheme performance is dependent on the network on which it is implemented. In fact, even the ranking of performance changes from one network to another, i.e. the best performing scheme in one network is not necessarily the best performing scheme in another network. Our results show how the identified factors contribute, both individually and collectively, to the PPM-based schemes' performance in large scale networks. Additionally, we find that when the networks are arranged in superfamilies, the networks within each superfamily exhibit similar scheme performance despite being created using different mathematical models and parameter values. Furthermore, we find that actual scheme performance far exceeds its theoretical upper bounds as derived from previous analytical models.

To complement our results, we present an analytical model that shows how the motifs exhibited by a network topology possibly affect the performance of PPM-based schemes in that network. This model explains the link between network superfamilies and scheme performance that is observed in our results. We also analyze and perform simulations on three extra networks directly derived from the Internet as described by the Caida project [42].

This work raises questions about the network dependency of other network protocols. Does the performance of other network protocols also vary from one type of network to another? If so, how can researchers guarantee that just because one protocol performs better than another in a given simulation network it will perform better in all other simulation networks or even in the Internet? This work and these questions therefore encourage multiple network evaluation of network protocols. To this end, our work demonstrates a method of identifying structurally similar Internet-like networks among which any protocol's performance is potentially comparable. If a protocol is proven to be linked to network superfamilies, network evaluation need only be done on representatives of each superfamily as opposed to all possible networks.

### **1.3 Dissertation Contributions**

In this section, we outline the contributions of this dissertation.

1. An analysis of PPM-based schemes is presented in Section 2.2 in which we extensively discuss the differences among selected existing PPM-based schemes. In particular, we discuss the differences among their underlying topologies and why the current approaches to network simulation are inadequate.

2. We present a novel PPM-based scheme called the Prediction-Based Scheme (PBS) in Chapter 3. The PBS scheme consists of independent marking and reconstruction algorithms that deal with data loss problems exhibited by previous schemes and exhibit comparatively lower convergence times.
3. We evaluate and compare the performance of selected schemes on an extensive set of Internet-like topologies and show how scheme performance, and even the ranking of performance, changes from one network to another. Our results show that scheme evaluation on a single network is not only inadequate but misleading as well.
4. We identify three network-dependent factors that affect scheme performance and contribute to the discrepancy in scheme performance exhibited among various networks in Section 4.2. We show the individual influence of these factors on scheme performance empirically.
5. Network motifs and subgraph ratio profiles are employed to identify superfamilies in a set of topologies. Each superfamily consists of networks that have similar local graph structure even when the networks are derived from different mathematical models.
6. We show a link between network motifs and the performance of PPM-based schemes analytically in Chapter 5. Our analytical model explains the influence of the network motifs on scheme performance.
7. We demonstrate a network clustering process that can be used to group Internet-like networks into superfamilies according to their structural similarity in Section 4.3. This allows researchers to evaluate network protocols on a smaller set

of representative networks as opposed to a large set of all possible simulation networks.

#### 1.4 Definitions and Terminology

In this section, we discuss terms that are central to the discussion in this dissertation. Some of these terms are described further where first encountered in this dissertation.

**Marking Scheme:** An approach to IP traceback that consists of a *marking algorithm* and a *traceback algorithm*. The marking scheme allows a victim of a flooding style DDoS attack to identify the attack sources. In the context of this dissertation, we use the term marking scheme to refer to the marking schemes that are based on the technique of Probabilistic Packet Marking introduced in [38] by Savage *et al.*

**Marking Algorithm:** An algorithm implemented at network routers that ensures each router randomly selects packets from its input traffic stream and embeds that router's identity into the identification field of the packet header before forwarding those packets onto their destinations. Because the marking algorithm is the primary component of the marking scheme, the marking algorithm is sometimes referred to as the marking scheme by researchers.

**Reconstruction Algorithm:** An algorithm implemented at the victim that uses the routers' identities embedded in any received attack traffic packets to build a graph representing the routers and edges traversed by attack traffic from its sources to the victim. The reconstruction algorithm is also referred to as the *traceback algorithm*.

**Convergence time:** The average number of network packets that a victim would have to receive during a DDoS attack in order to reconstruct the complete attack graph successfully and consequently identify the attack sources.

**Packet:** A network packet is a basic unit of data being transmitted across a network such as the Internet. It consists of a packet header which contains control information, and a payload which contains the user's data. In PPM-based schemes, router identities are potentially embedded in the identification field of the packet header.

**Attack path:** A collection of nodes and edges linking a single attack source to the victim. It represents the path that the traffic from that source traversed in order to arrive at the victim.

**Attack graph:** A collection of nodes and edges linking all the sources of a DDoS attack to the victim. The attack graph represents all the routers and edges that were involved in forwarding the attack traffic from its sources to the victim.

**Node:** A component of an attack path/graph that represents any device operating at the Internet layer of the TCP/IP model or the network layer of the OSI model (e.g. routers, switches, hosts).

**Edge:** A component of an attack path/graph that represents a direct link between nodes. Two nodes are connected by an edge if Internet traffic can be transmitted directly between them without being forwarded by any intermediate nodes.

**Upstream router:** Given that the attack traffic flows from an attacker to the victim, an upstream router refers to any router in an attack path that is located closer to the attacker. The term is typically used in comparison to a downstream router.

**Downstream router:** In contrast to the upstream router, a downstream router refers to any router in an attack path that is closer to the victim.

**Subgraph:** In the context of this dissertation, a subgraph refers to a connected graph which is a subset of a larger network. The subgraphs considered in this work consist of four nodes with undirected edges.

**Network motif:** A network motif is any subgraph in a given network that is significantly prevalent. The subgraph's level of prevalence is derived by comparing its frequency in the network with its frequency in similar randomized networks.

**Subgraph ratio profiles:** A form of "signature" for a network that represents the relative frequency of a given set of subgraphs in that network. Networks with similar subgraph frequencies for all considered subgraphs will typically exhibit similar *subgraph ratio profiles* (SRPs).

**Superfamily:** A collection of networks that exhibit similar SRPs. Networks originating from different fields of science or created using different mathematical models could potentially belong to the same superfamily. In contrast, networks created using the same mathematical models or originating from the same field of science could potentially belong to different superfamilies.

**Alternative path/route:** More than a single route between a source and a target. In the context of an attack graph, an alternative route suggests that the attack traffic from a single source traversed more than a single path to arrive at the victim, i.e. one portion of the traffic traversed one path, and another portion traversed a different path. In the context of a subgraph, alternative paths means that it is possible to select two nodes from a subgraph, between which exists more than one unique path.

If such a subgraph were situated within an attack graph, that attack graph would exhibit alternative paths.

### **1.5 Organization of the Dissertation**

In Chapter 2, we discuss various PPM-based schemes and highlight the weaknesses that are addressed in this dissertation. In Chapter 3, we present the Prediction-Based Scheme and results showing how it compares to selected PPM-based schemes in different attack graph scenarios. We discuss the network dependency of PPM-based schemes, the identified network dependent factors, and the network classification approach herein implemented in Chapter 4. In Chapter 5, we discuss the traditional analytical model, and present our proposed extensions to that model. Chapter 6 contains a study of our simulations, and the results of the network dependency study are discussed in Chapter 7. We then present concluding thoughts in Chapter 8.

## CHAPTER 2

### BACKGROUND AND RELATED WORK

#### 2.1 A Background on PPM-Based Schemes

The field of IP traceback consists of a variety of schemes designed to find the origin of Denial of Service (DoS) attacks. Most of these schemes have experienced limited success in the industry as evidenced by their low levels of deployment by Internet Service Providers (ISPs) [54] and yet DDoS attacks are still a prevalent problem today [45, 18, 5, 6, 7]. Schemes have to be designed with an eye on their deployment feasibility in order to encourage ISPs to use them. IP traceback schemes can be categorized according to attributes such as a principle, processing mode, or location [9]. When classified according to principle, IP traceback schemes fall into one of two broad categories: those that employ logging and those that employ marking.

In marking schemes, some or all the routers along the path between an attacker and victim (attack path) send information about themselves or adjacent edges in the path to the victim. When the victim obtains sufficient information, the entire attack path can be reconstructed [9]. This information can be sent as an extra packet, as in ICMP based traceback, or embedded within the packet itself, as in Probabilistic Packet Marking (PPM) based techniques.

PPM-based schemes consist of a *marking scheme* and a *reconstruction procedure*, and are based on the assumption that large amounts of traffic are used in a (D)DoS attack [38]. In their original work, Savage *et al.* [38] propose that the PPM marking scheme is employed at all times in all the routers in the network, while the reconstruction procedure is employed by the victim in the event of an attack. The marking scheme ensures that every router embeds its own identity in packets randomly selected from the packets the routers process during routing. Since a large number of packets is received in an attack, there is a considerable chance that a victim will have received packets with markings from all the routers that were traversed by the attack packets. The victim then employs the reconstruction procedure which uses the received marked attack packets to map out the *attack graph* – the paths from the victim to the attackers. The total number of received packets required to trace the attackers is referred to as the scheme’s *convergence time*. One advantage of PPM-based schemes is that they do not require much ISP involvement and are effective for DoS attacks. However, they typically do not scale well for DDoS attacks and are susceptible to spoofed markings [9]. The family of PPM-based schemes consist of the many adjustments to the primitive form of PPM that attempt to tackle its weaknesses as well as improve its strengths [51, 49, 39].

One example of a PPM-based scheme is the *Tabu Marking Scheme* (TMS) [30]. The author points out that PPM is prone to information loss as a result of *re-marking*. Re-marking occurs when a router randomly selects a packet which already has marking information from an upstream router, and consequently overwrites this information. TMS tackles this problem by ensuring that their marking scheme forfeits the marking

opportunity in the event that the randomly selected packet contains previous marking information. As a result, they report lower convergence times than PPM for DDoS attacks.

Another one of these improvements is with the Advanced and Authenticated Marking schemes (AMS) presented by Song *et al.* [39]. These marking schemes support incremental deployment, which means that they are still successful even if they are not implemented on all the routers in the network. They also scale better to handle DDoS attacks because of lower computation overhead. They improve efficiency by utilizing a predetermined or previously obtained map of upstream routers. With this information, the traceback scheme does not require as many packets for traceback and therefore tracing DDoS attacks is more computationally feasible.

Wong *et al.* [49] present the Rectified Probabilistic Packet Marking (RPPM) traceback algorithm to be used with the PPM. They point out that the reconstruction procedure used in PPM-based schemes has an imprecise termination condition. Typically, the analytical model in [38] is used to predict how many packets are required, but the model depends on the attack path length which is not known before the reconstruction is complete. Because the convergence time is considerably less than the total number of packets received during a typical attack, the victim is generally sure that the attack graph will be complete after analyzing all the received packets. However, a problem arises during short term attacks because the victim cannot tell if extra unique edges would be identified by receiving more packets. The authors present a mathematical formulation for a precise termination condition that enables complete attack graph reconstruction within a user-specified level of confidence.

In the next chapter of this dissertation, we present an alternative scheme called *Prediction-Based Scheme* (PBS) which also avoids re-marking [26]. However, in contrast to TMS, the PBS marking scheme ensures that the router information is embedded in the next available packet if the randomly selected packet already has marking information. The PBS marking scheme requires extra space cost of one bit compared to PPM. Additionally, the reconstruction algorithm utilizes both legitimate and attack traffic to reconstruct the attack graph. The PBS reconstruction algorithm is an extension of the RPPM reconstruction algorithm in [49].

Many other schemes have been proposed to increase the efficiency of PPM in different ways e.g. [51, 36, 23, 52]. Some of these schemes are presented in Table 2.1. The table compares our approach to nine other PPM-based schemes in terms of features such as convergence time, underlying topologies, incremental deployment, re-marking, and upstream graph.

The *convergence time* refers to mathematical analysis for a single path scenario under uniform marking probability  $p$  and path length  $d$ . The expressions capture how many packets it would typically take to identify the entire path linking the victim to an attacker.

The feature *incremental deployment* refers to whether the scheme would be successful if the marking scheme is deployed on a fraction of the routers in the network. Only a few schemes explicitly state that they would be successful when partially deployed [38, 39, 51, 23]. Incremental deployment means partial attack graph reconstruction is possible even when some ISP's in the attack graph have not implemented the marking scheme on their routers.

**Table 2.1:** A comparison of 10 different PPM-based schemes over their features. These features include *convergence time*, whether they require prior knowledge of the *upstream graph* to correctly identify attackers, whether they can be *incrementally deployed*, and *underlying topology*. The convergence time expressions presented in the table are for a DoS scenario assuming no prior knowledge of the network topology while the underlying topology shows the network topologies used in the evaluation of the schemes. These topologies include *single path, single attacker* (SP/SA), *single path, multiple attacker* (SP/MA), and *multiple path, multiple attacker* (MP/MA)

Scheme	Year	Convergence time	Incremental deployment	Re-marking	Upstream graph	Underlying topology
PPM [38]	2001	$\leq \frac{\ln(d)}{p(1-p)^{d-1}}$	yes	yes	no	SP/SA (max. 30 hops)
AMS [39]	2001	<i>undetermined</i>	yes	yes	yes	Traceroute data set (103402 destinations, 2000 attackers)
PPM-NPC [44]	2004	$\leq \frac{\ln(d)+0.58}{p}$	no	no	no	SP/SA (10 hops)
TMS [30]	2005	$\leq \frac{\ln(d)}{p(1-p)^{d-1}}$	no	no	yes	Binary tree (6 hops, 32 sources)
FIT [51]	2005	<i>undetermined</i>	yes	yes	yes	Skitter map (174409 hosts, 5000 attackers)
RPPM [49]	2008	$< \frac{\ln(d)}{p(1-p)^{d-1}}$	no	yes	no	SP/SA, binary tree, random tree network (15, 100, 500, 1000 nodes)
TPM [36]	2008	<i>undetermined</i>	no	yes	yes	Skitter data (avg. 18 hops)
Randomize-and-link [23]	2008	$< \frac{nH_n}{p(1-p)^{d-1}}$	yes	yes	no	Binary tree (10 hops)
IDPPM [52]	2010	<i>undetermined</i>	no	yes	no	SP/SA (20-32 hops)
PBS [26]	2012	$\leq \frac{\ln(d)}{p}$	no	no	yes/no	SP/SA, SP/MA, MP/MA, 50 node network, 100 node network

*Re-marking* refers to whether the marking scheme at a router permits the overwriting of the previous edge or router information in a packet. The majority of the considered schemes permit re-marking of packets [38, 39, 51, 49, 36, 23, 52]. The packet selection process at the routers that implement these schemes is completely random, which means that it is possible for a router to randomly select and consequently re-mark a packet that already has marking information from an upstream router.

*Upstream graph* refers to whether a scheme requires a previously obtained map of the network to successfully trace the specific path taken by attack traffic. Some of the works address how such a map can be obtained to aid in attack graph reconstruction [39, 51, 26]. Access to the map of a network allows for significantly improved performance since sections of the attack path can be inferred as opposed to being identified explicitly.

The *underlying topology* shows the different network topologies that are used for simulation purposes in those papers. The results from these topologies are used to provide an indication of how the schemes would perform if implemented in the Internet. More discussion of this feature is provided in a subsequent section.

The schemes considered therein are by no means an exhaustive study of all the PPM-based schemes in existence. However, the collection of schemes is large enough to show the discrepancy in underlying topologies, which makes them inadequate for direct comparison of scheme performance.

It is important to point out that PPM-based schemes are not the only proposed approaches to IP traceback [9, 22]. Alternatives include packet logging [29], specialized routing [40], Internet control message protocol (ICMP) traceback

[10], deterministic packet marking [8], and hybrid approaches which combine different traceback techniques [53] or combine traceback with anomaly detection [50].

We have been able to publish various portions of the work in this dissertation in [26, 27, 28].

## 2.2 Underlying Topologies and PPM-Based Schemes

In this section, we discuss the relationship between the underlying topologies used for simulation purposes and the PPM-based schemes. It contains the background research considered for the topology dependence study presented in the second part of this dissertation.

### 2.2.1 A Comparison of Previous Underlying Topologies

Ideally, the performance of a network protocol such as a PPM-based traceback scheme would be evaluated on either the Internet itself, or a topology exactly like it. By simulating the schemes on an underlying topology, researchers are able to understand the performance of those schemes. The simulations also allow researchers to validate any derived analytical models and show how any scheme would perform in a network such as the Internet.

However, because the Internet is enormous, dynamic and heterogeneous, attempts to carry out empirical protocol evaluation are expensive and inflexible [13]. As a result, researchers resort to simulations implemented on underlying topologies which are considered to be simplified abstractions of the topology of the Internet [13, 41, 20, 32]. In this case, an underlying topology is represented by a graph  $G(v, e)$  consisting of nodes  $v$  and edges  $e$  where the nodes represent either devices with routing

capability or end hosts. An edge between any two nodes means that traffic can be directly transmitted between those two devices [13].

It is important to point out the difference between a network topology and a routing topology and how this difference affects our work. A *network topology* consists of all nodes in a network and all the edges between those nodes. It represents all possible routes that network traffic can use to get from any point in the network to any other point. On the other hand, a *routing topology* consists of the nodes and edges that traffic typically traverses to get from one point in the network to another. Since the routing topology only captures typical traffic routes, it is a subset of the network topology. In this section, we show that while traditional underlying topology choices are appropriate for routing topologies, they make inadequate network topologies. Using a routing topology as an underlying topology assumes that attack traffic will always take typical traffic routes even under the duress that a DDoS attack exposes the network to.

A typical simulation is carried out as follows. During set up, the marking algorithm is implemented in the nodes (routers) of the underlying topology. To simulate the attack, packets are transmitted from one or more nodes (representing the *attackers*) to one specific node (representing the *victim*). A reconstruction procedure is then implemented at the victim to map out the attack graph  $G_{act}$ . The resulting attack graph should consist of only the nodes and edges in the underlying topology that were directly involved in transmitting the attack packets.

As shown in Table 2.1, a variety of underlying topologies have been used to evaluate the performance of PPM-based schemes. The underlying topologies used range from simplistic to complex, as described below.

The *single path, single attacker* (SP/SA) is a simple topology consisting of a single attacker node sending packets along a single path to a single victim node. The length of the path varies with each work ranging from 3 hops to 32 hops [38, 49, 26, 44]. This setup is used to simulate the performance of PPM schemes during a flooding style DoS attack.

The *Single Path, Multiple Attacker* (SP/MA), and *Multiple Path, Multiple Attacker* (MP/MA) topologies consist of multiple sources of attack traffic to simulate a DDoS attack. The SP/MA simulates a unique topology in which all the attackers are located at different distances from the victim but all along a single path [26]. The MP/MA simulates a more general topology where each attacker has a unique path linking it to the victim node. In some cases, the paths are completely independent [49], while in other cases, the paths merge closer to the victim [30, 49, 23, 26].

One unique MP/MA topology is a tree, e.g. a binary tree. In this case, the attack graph is modeled as a tree with some or all of the leaves at a certain depth representing the attack nodes, and the root of the tree representing the victim node [30, 49, 23]. This setup ensures that different attack paths merge the closer they are to the victim. As with SP/SA and SP/MA, there is only one path in the attack graph from an attack node to the victim node.

Some authors have evaluated their schemes using actual data sets from the Internet [39, 51, 36]. These include traceroute data sets from Lucent Bell labs in [39]

and CAIDA’s skitter map in [51, 36]. These data sets are used to produce topologies that are typically larger than the simple topologies mentioned thus far and provide better abstractions of the Internet structure. In this work, we have included three complementary Caida networks into our network set to provide a form of comparison for the rest of the network set.

One common feature with these underlying topologies is their tree-like structure. A tree-structured topology  $G_{tree}$  exhibits a single path from any given attacker to the victim. The choice of tree-structured topologies is based on the assumption that all attack traffic from one attacker will take the same path to the victim. This assumption is in turn based on the observation that Internet paths are largely invariant particularly over short periods of time [37]. These assumptions have allowed researchers to simplify the simulation process by ignoring the routing and load balancing capabilities of the network and enforcing a predefined (or pre-observed) set of paths for attack traffic. However, the prevalence of load balancing routers in the Internet today [2, 17] makes the assumption of a tree-structured topology an unrealistic one. Augustin *et al.* report that 39%-70% of the routes measured in [2] exhibit route fluttering as a result of load balancing. Load balancing routers frequently forward traffic along alternative paths in order to minimize cost to the network. Consequently, scheme performance in tree-structured topologies, where all traffic from one source takes one path, cannot be used as an indication of how those schemes would perform in Internet-like network topologies.

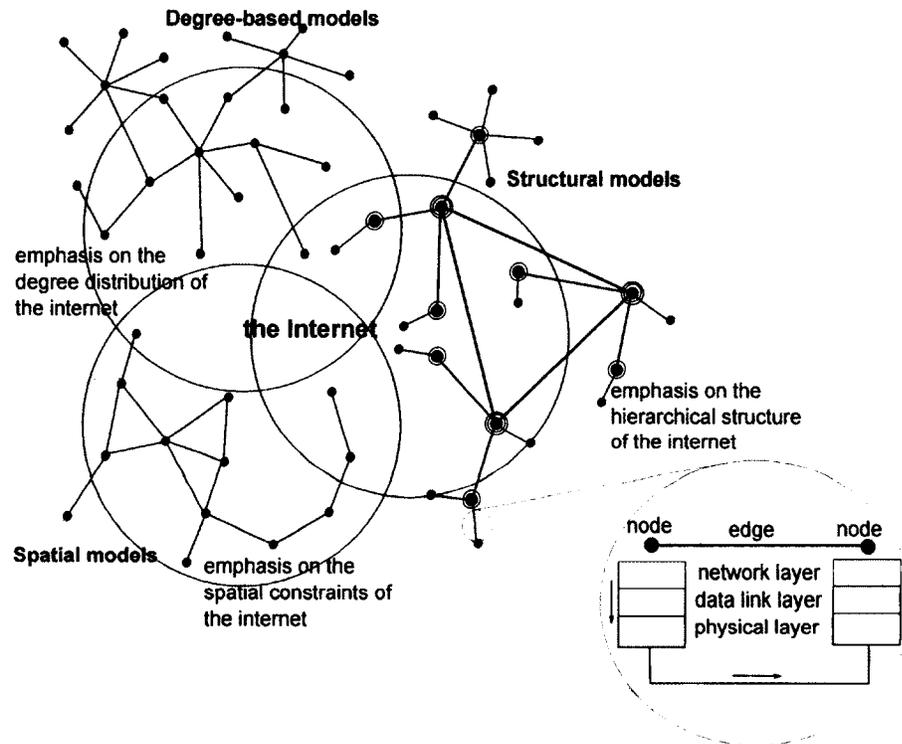
During our initial evaluations of PBS, we considered two well-connected albeit small networks [26]. In contrast to the tree-like networks ( $G_{tree}$ ) typically considered

in PPM-based schemes, well-connected networks contain alternative routes between attackers and any victim. Simulations carried out in well-connected networks, where routers make routing decisions as well as marking decisions, more closely capture the performance of the schemes if they were deployed in the Internet. In this work, we follow up by considering a larger number of network models to investigate the marking schemes.

We consider the models that have been shown to simulate the Internet topology [13, 41, 46, 16, 47]. These models fall into three categories based on the Internet properties that they emphasize, namely degree-based models, structural models and spatial models (cf. Figure 2.1). The emphasis of degree-based models is the degree distribution of the nodes in an attempt to recreate the power law observations in the Internet [20, 47]. The structural models arrange the nodes to mimic the hierarchical structure of the Internet, with Internet traffic being transmitted through routers located within autonomous systems [13, 32]. The spatial models place emphasis on the location of the nodes with any two nodes being connected only if they are within a transmission range of each other [16]. The three categories of models are used to create 60 Internet-like topologies which are then used to provide a clearer picture of the performance of PPM-based schemes in an Internet-like environment.

Using mathematical models to create underlying topologies for simulation allows us to link scheme performance to the structural characteristics exhibited by a category of networks. For example, a pattern in scheme performance in the degree-based networks (such as the Barabasi and Waxman networks) could be potentially linked to the power law in the Internet. In contrast, a pattern in the structural networks (such

as the Top-Down hierarchical networks) could be linked to the hierarchical structure of the Internet. An actual Internet topology dataset would not lend itself easily to such analysis because it exhibits all these characteristics and therefore attributing scheme performance to one specific characteristic would be more difficult.



**Figure 2.1:** Internet topology can be captured by a variety of models which include spatial, structural and degree-based models. Each model emphasizes different properties of the Internet and can be used to evaluate network protocols when employed in the Internet. The nodes in these topologies represent devices operating at the Internet layer of the TCP/IP model or the network layer of the OSI model (e.g. routers, switches, hosts). Two nodes are connected by an edge if Internet traffic can be directly transmitted between them without being forwarded by any intermediate nodes.

Despite the convenience and prevalence of using mathematical models for the Internet, we must point out that they do not provide a completely accurate description of the Internet topology. The process of capturing and modeling the topology of the

Internet is not only a complex process but is also an ongoing one with many unresolved challenges, the details of which are beyond the scope of this dissertation. However, the network set used in our work is sufficient for the purposes of comparing scheme performance, and providing a benchmark for further studies about scheme dependence on topologies.

### 2.2.2 Selecting Representative Marking Schemes

Table 2.1 shows that the different schemes contain different features that help to improve their performances in one way or another. Therefore, to facilitate the comparison of the different marking schemes in our simulations, it is imperative that the schemes are evaluated on the same “level”. The level selected for the uniform comparison of the schemes is their underlying algorithms. By considering the underlying algorithm, we disregard environment specific features such as router identity fragmentation, network dependent implementation details, and different confidence levels in attack graph construction. Consequently, we are able to categorize the marking schemes according to their underlying algorithms, and then select representative schemes from each category for simulation purposes. Additionally, we do not consider external factors such as complementary network traffic and traffic dynamics. As a result of these adjustments, the obtained results should not be taken as an absolute measure of the scheme performance in all networks, but rather used as a relative measure between different schemes and/or different networks.

Despite their large number, PPM-based schemes have similar underlying algorithms in their marking schemes. The underlying algorithm is responsible for how

the packets, in which the router identities are embedded, are selected. For example, the majority of the considered schemes exhibit underlying algorithms in which all routers randomly select packets with equal probability  $p$  [38, 39, 51, 49, 36, 23, 52]. The schemes in this category are prone to re-marking. We refer to this category as the re-marking category of PPM-based schemes. In the other category of schemes, the routers' packet selection process is only partially random. The underlying algorithms in this category prohibit the overwriting of previous router information and as a result exhibit performances that are notably different from the re-marking category [44, 30, 26].

We select three representative marking schemes: PPM [38] to represent the re-marking category, and TMS [30] and PBS [26] to represent the non-re-marking category. The analytical models for these three schemes are markedly different from each other, even for equal marking probability, because of the differences in the schemes' underlying marking algorithms, and yet representative of their respective categories. The performance of any PPM-based scheme can therefore be compared to either one of these schemes, or a combination of them.

Because of re-marking in PPM, the victim typically receives more markings from close-by routers than from distant routers. The chance of receiving a marked packet from a router  $l$  hops away is given by the geometric distribution expression  $p(1 - p)^{l-1}$ . This is because a received marked packet indicates that that packet was selected by a router (with probability  $p$ ), and not selected (with probability  $1 - p$ ) by all  $l - 1$  subsequent routers. The analysis for PPM can therefore be applied to

any scheme where the markings from distant routers are rarer than markings from close-by routers.

In TMS, the decision to forfeit a marking opportunity if the packet is previously marked means that markings from routers distant from the victim are more prevalent than markings from closer routers. The chance of receiving a marked packet from a router  $l$  hops away is given by  $p(1 - p)^{d-l}$  where  $d$  is the attack path length. This is because a received marked packet indicates that that packet was selected by a router (with probability  $p$ ), after not being selected (with probability  $1 - p$ ) by all  $d - l$  previous routers. This analysis can be applied to all schemes in which markings from distant routers are more prevalent than markings from close-by routers.

In contrast to TMS, the PBS marking scheme compensates for the missed marking opportunities. Therefore, the chance of receiving a marking from a router  $l$  hops from the victim is given by  $p$  for any router in the path. This analysis can be applied to all schemes in which the markings from the routers are equally prevalent regardless of their distance from the victim. Understanding the impact of network topology on these three schemes therefore provides an adequate basis to understand the impact of network topology on other PPM-based schemes.

### 2.3 Using Subgraphs to Differentiate Networks

Milo *et al.* [34] introduce the concept of *network motifs* to compare arbitrary network topologies. In their seminal paper, network motifs are defined as the significantly prevalent subgraphs exhibited by a network. By identifying 3-node and 4-node motifs, it is possible to establish structural similarities among different

networks ranging from electronic circuits, to neuron synaptic connections, to ecological food webs, to world-wide web hyperlinks, e.t.c. They argue that the network motifs are the fundamental building blocks of the networks, and as such, different networks can be compared by using them. Furthermore, the motifs are used to understand the underlying functions that generate each network.

Milo *et al.* [33] follow up this work by using 3-node and 4-node subgraphs to create “signatures” for different networks from different fields of science. The signatures are based on the relative abundance or absence of the subgraphs which in turn are evaluated by comparing those networks to randomized networks of the same size and connectivity. These signatures, referred to as *subgraph ratio profiles* (SRPs), are then compared among networks and used to assign the networks to *superfamilies* based on their similarities. Networks in the same superfamily are understood to exhibit similar underlying structure regardless of their generation principles or the fields of science from which they came.

Network motifs and SRPs have since then been used to compare different networks from fields such as social networks [55], neural networks [48], cooperative networks [24], protein interaction networks [19], and gene-regulation networks [15]. Additionally, some work has been done in improving the time efficiency of the process of counting network motifs [31]. To the best of our knowledge, our work is the first where the technique has been specifically adapted to identify the superfamilies in Internet-like networks.

## CHAPTER 3

### PREDICTION-BASED SCHEME

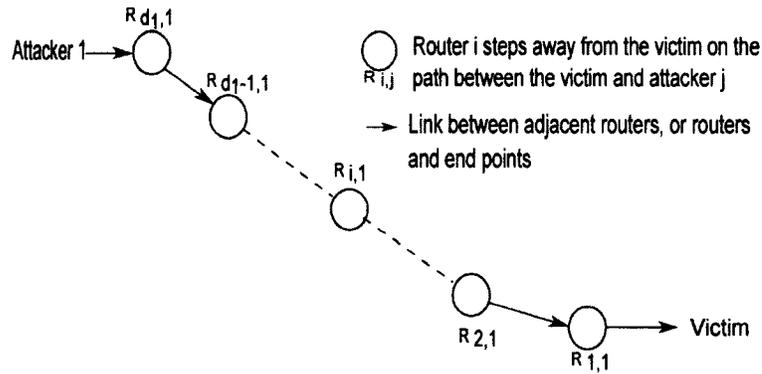
#### 3.1 Problem Statement and System Model

The general process of tracing an attacker using PPM is outlined below.

1. Before an attack, a *marking scheme / algorithm* should be implemented in the routers of a network. The marking algorithm allows each router to select a packet in its processing queue and embeds its router identity in that packet regularly.
2. During an attack, the victim collects all attack packets.
3. Either during or after the attack, the victim employs a *traceback algorithm* that searches through the collected packets to find markings indicating what routers (or edges) the packets traversed.
4. The traceback algorithm returns a graph showing how all the routers in the attack path are connected to each other based on the received packet markings. It returns a complete attack graph if all routers in the graph have been identified.

Implementation of a marking scheme is the primary step of the traceback process, and the algorithm used for the marking affects the efficacy in which traceback can be accomplished.

An example is shown in Figure 3.1, in which there is a single attacker (Attacker 1) sending  $N_1$  number of attack packets, along a path of  $d_1$  routers between the attacker and the victim. We refer to this topology as the *Single Path, Single Attacker (SP/SA)* topology throughout this paper. Each router in the attack path independently selects whether to mark the packets going through it with probability  $p$ . It follows that there is a probability  $(1 - p)$  that any packet going through a router in the path will not be marked by that router.



**Figure 3.1:** *Single Path, Single Attacker (SP/SA)*

In PPM, the majority of marked packets received by the victim are from routers close to the victim. This is because the traditional PPM marking algorithm allows overwriting of marking information. Any marking information embedded in a packet by a router can be potentially overwritten by another router downstream in the path to the victim. This happens when the same packet is randomly selected by more than one router along its journey, causing the loss of information from the upstream routers. For any router marking to be received by the victim, the marked packet should not be marked again by any subsequent routers that it passes through. The

marking problem can be modeled as a binomial problem with *success* defined as *being marked by a specific router*. Given that a router is  $i$  hops away from the victim, the probability of that router's markings reaching a victim is a product of one success  $p$  and subsequent failures  $(1 - p)^{(i-1)}$ . The expression  $Np(1 - p)^{(i-1)}$  describes the number of attack packets received by the victim, which are marked by that router, if the attacker sends  $N$  packets that all take a single path. Assuming the router sent  $Np$  packets with its information, the factor  $(1 - p)^{(i-1)}$  accounts for information that is lost due to remarking of packets by subsequent routers.

Extending this analysis to  $k$  attackers and  $k$  paths (assuming that the packets from one attacker follow a single path to the victim<sup>1</sup>), the number of packets marked at distance  $i$  from the victim is described by the general expression in Equation 3.1. Hereby, each attacker  $j$  sends  $N_j$  packets:

$$\sum_{j=1}^k N_j p (1 - p)^{i_j - 1}; \quad 0 < i_j \leq d_j. \quad (3.1)$$

The Tabu marking scheme [30] provides an alternative to the marking scheme. To compensate for the loss of information, the scheme is implemented such that a packet randomly chosen for marking by a router is not remarked if it already has marking information from a previous router. This ensures that information from upstream routers is not overwritten by downstream routers. However, this guarantee comes at the cost of losing potential marking information from downstream routers. By prohibiting remarking, a router forfeits the chance to embed its own marking information in a previously marked packet. As a result, the majority of marked

---

<sup>1</sup>Under this assumption, it is possible for more than one attacker to have the same path.

packets received by the victim are from more distant routers. The number of attack packets received that are marked by a router  $i$  hops away from a victim in an attack path of length  $d$  can be modeled binomially as a product of one success  $p$  and prior failures  $(1 - p)^{(d-i)}$ . This is because the marking from router  $i$  will only get to the victim if the packet that was chosen for marking has not been chosen previously by upstream routers. The number of marked packets from the router  $i$ , given one attacker who sends a total of  $N$  packets along one path, is described by the expression  $Np(1 - p)^{(d-i)}$ . Given that each router had the potential to send  $Np$  packets with their own information, the factor  $(1 - p)^{(d-i)}$  accounts for the possible information that is lost due to not remarking the packets.

Similarly, for the general case of  $k$  attackers and  $k$  paths, the number of packets marked at distance  $i$  from the victim is given by the general expression in Equation 3.2:

$$\sum_{j=1}^k N_j p (1 - p)^{d_j - i_j} ; \quad 0 < i_j \leq d_j. \quad (3.2)$$

Conclusively, PPM schemes that allow overwriting lose information from earlier routers, while Tabu that does not allow overwriting loses possible information from latter routers.

We propose a marking scheme that loses information from neither earlier nor latter routers. The resulting expression for attack packets received marked by a router  $i$  steps away from a victim is given by  $Np$  for the SP/SA scenario and is therefore independent of the distance from the victim.<sup>2</sup>

---

<sup>2</sup>The number of marked packets received is independent of  $i$  for most practical ranges of  $p$  and  $d$ . We define a “saturation condition” later on in this document, where this independence fails.

For the general case of  $k$  attackers and  $k$  paths, the number of packets marked at distance  $i$  from the victim is given by the general expression in Equation 3.3:

$$p \sum_{j=1}^k N_j ; \quad \forall i_j \geq d_{min} - \frac{1}{p}. \quad (3.3)$$

Step 4 of the PPM traceback process is an expensive step in terms of time and processing power. It is during this step that the attack graph is reconstructed and the attack sources are identified. In this graph, the nodes are the routers, and the edges are the links between the routers. The routers in the attack graph will include the subscriber edge routers directly connected to the attackers and/or victim, and all the routers in between. Traditional traceback algorithms seek to identify all routers in the attack graph at distance  $d$  from the victim before identifying routers at distance  $d + 1$ . This approach is not effective with insufficient information about routers at distance  $d$ , because the algorithm cannot identify routers in the attack path farther than that. Since the aim of traceback is to identify one or more leaves in the attack tree, a missing edge is a dead end in traditional traceback algorithms. The extension to the traceback algorithm in PBS seeks to avoid this dead end by using graphs built using legitimate traffic. This adjustment makes tracing the multiple attackers of a DDoS attack significantly faster.

The Prediction-Based Scheme (PBS) is based on two ideas and on known PPM techniques. First, the marking routine is similar to the traditional PPM Scheme except that if a router selects a packet that already has router information, it marks the *next available packet* with its information. By *next available packet*, we refer to a packet further on in the processing queue of the router without any marking

information. This exposes the scheme to spoofing, where attackers insert erroneous router information because this wrong information will not be overwritten and will arrive at the victim and frustrate any traceback attempts. To deal with this, we propose that all edge routers that employ the scheme clear the IP identification field of all packets passing through the routers, hence removing any false information put there by the attacker prior to the packets entering the network. Second, the traceback algorithm leverages legitimate traffic collected before or after the attack to complete any missing edges in the attack graph and consequently shorten the reconstruction process.

### 3.2 Our Approach: Prediction-Based Scheme

The proposed Prediction-Based Scheme (PBS) is based on two novel ideas to complement traditional PPM techniques, i.e. a marking scheme, and a traceback algorithm. The marking scheme can be used with other traceback schemes, while the traceback scheme can be used with other marking schemes to yield improvement.

#### 3.2.1 PBS: Router Marking Algorithm

The marking scheme is similar to the traditional PPM scheme except that, if a router selects a packet that already has router information, it marks the *next available packet* with its information. By *next available packet*, we refer to a packet further on in the processing queue of the router without any marking information. This ensures that previous marking information is not lost by overwriting. The marking algorithm is described in Figure 3.2.

Each router has a boolean variable that we refer to as the *router\_variable* that is *false* as a default value. Upon receiving a packet, a router checks the state of its *router\_variable* and deals with the packet differently depending on that state.

If the *router\_variable* is *false*, the router generates a random floating point number  $w$  in the range  $[0, 1]$ . If this number is below the marking probability  $p$ , then the packet has been selected for marking.

Upon random selection, the router then proceeds to check whether this randomly selected packet has any previous router information embedded in it. If it does not, then the router embeds its own identity into the packet and forwards the packet to the next router. However, if the packet has previous routing information, the router changes its own *router\_variable* to *true*, and then forwards the packet without changing any of the information in it.

If the *router\_variable* is *true*, every received packet will be inspected for previous router information. When a packet is found that does not contain any previous router information, the router identity is embedded in that packet, and the *router\_variable* is set back to *false*.

```

Input: network packet and router_variable
/* router_variable is a boolean variable with the default value of
  FALSE                                                                    */
Output: Marked Network Packets
foreach Packet do
  if (router_variable == TRUE) then
    if (packet is already marked) then
      | set router_variable to TRUE ;
      | increment distance;
    end
    else
      | mark packet;
      | set distance to 0;
      | set router_variable to FALSE;
    end
  end
else
  /* router_variable == FALSE                                                                    */
  select random number w where  $w \in [0, 1]$ 
  if ( $w \geq p_{recommended}$ ) then
    | /* packet was not selected for marking.  $p_{recommended} = 0.04$  */
    | increment distance;
  end
  else
    /* packet has been randomly selected for marking */
    if (packet was marked by earlier routers) then
      | set router_variable to TRUE;
      | increment distance;
    end
    else
      /* packet is available for marking */
      mark packet;
      set distance to 0;
      set router_variable to FALSE;
    end
  end
end
  forward packet;
end

```

**Figure 3.2:** Prediction-Based Scheme: The marking algorithm

The router increments every packet's distance field unless that packet was selected for marking. In that situation, the distance field is set to  $\theta$ . By avoiding overwriting, previous marking information is not lost. By marking the next available packet, the scheme ensures that every router will have  $Np$  marked packets. Hereby  $N$  is the total number of packets that pass through the routers, and  $p$  is the marking probability of the scheme.

One of the drawbacks to this scheme is *saturation*. During saturation, a router fails to find an available packet in which to embed its identity without overwriting previous router information. This typically happens for either high marking probability values ( $p$ ) or large route length values ( $d_j$ ). It results in fewer packet markings for routers closer to the victim.

An additional drawback to the scheme is vulnerability regarding spoofing. That is, if an attacker inserts erroneous router markings into the packets before introducing them to the network, those false router markings are not overwritten by routers that employ PBS and arrive uncorrected at the victim. To deal with this, we require that all routers at the edge of the network clear the marking field and set the distance to  $\theta$ . In that way, false router marks introduced by the attacker are removed before the packets enter the network.

### 3.2.2 PBS: The Traceback Algorithm

Traditional traceback algorithms have two main weaknesses. One weakness is they fail to identify an attack graph if there is missing information in the attack

packets. If one of the routers' or edges' identities is absent in the received marked packets, then the algorithm is unable to produce a complete attack graph.

Another weakness is that it takes a large number of packets to construct the complete attack graph. The algorithm would have to wait until it receives a sufficient number of packets such that the marked packets contain markings for all routers in the path. This problem becomes worse in DDoS attacks because the algorithm is tracing more attackers. Additionally, since the attack is comprised of more sources of attack packets, the attacker can afford to send fewer packets from each source making tracing back to any single source more difficult.

We solve these problems by adding a prediction component to the traceback algorithm presented by Wong *et al.* [49]. This extra component fills out the empty nodes/edges in the incomplete attack graph, resulting in traceback with fewer received packets. Prediction is possible because internet paths are dominated by prevalent routes which do not change significantly [37]. The prediction is done by using the packet statistics of legitimate traffic, which can be collected prior to or after the attack. The packet marking of legitimate traffic is used to build a legitimate graph that is later used to fill in the gaps in the attack graph. If an attack packet, marked by a router  $R_{i,j}$  which is also part of the legitimate graph, is received, then all packets marked by all routers  $R_{l,j}; l \leq i$  in between the victim and that router can be ignored. This is because it is possible to predict where that packet passed based on the legitimate graph. The traceback algorithm is described in Figure 3.3.

```

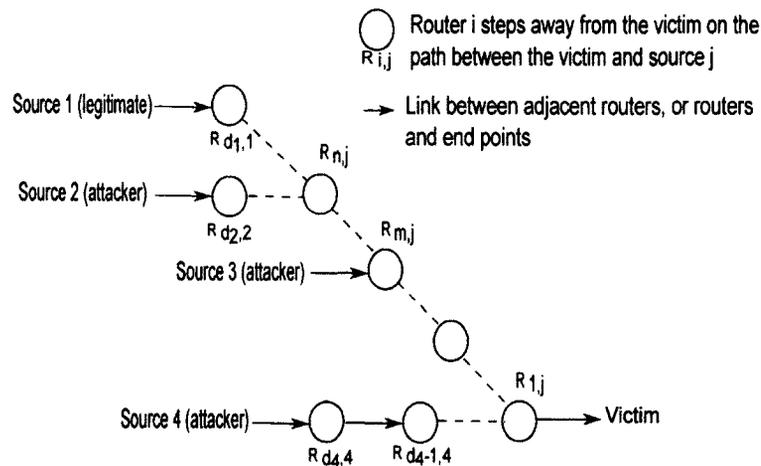
Input: network packet
/* Attack graph  $G_a$  contains just victim node,  $V$  initially, */
Output: Constructed Attack Graph
foreach Packet do
  increase packet_count
  if (packet contains an edge  $e$  in legitimate graph  $G_l$ ) then
    append legitimate subgraph  $G_{l(v \rightarrow e)}$  to attack graph  $G_a$  /*  $G_{l(v \rightarrow e)}$  consists
    of all nodes and edges from victim  $V$  up to edge  $e$  */
  end
  if (edge  $e$  is NOT contained in attack graph  $G_a$ ) then
    Insert edge  $e$  to graph  $G_a$ 
    if ( $G_a$  is a connected graph) then
      recalculate Termination_Number  $T$  /* The Termination_Number is
      recalculated using a subroutine that depends on the state
      of  $G_a$ . [49] describes such a subroutine */
      reset packet_count
    end
  end
  if ( $G_a$  is a connected graph) and (packet_count >  $T$ ) then
    return  $G_a$  as the attack graph
  end
end

```

**Figure 3.3:** Prediction-Based Scheme: The traceback algorithm

We illustrate our traceback algorithm using the *Single Path Multiple Attacker* (SP/MA) (cf. Figure 3.4), which links the victim to four possible traffic sources. In the figure, Source 1 is a legitimate source of traffic, while Sources 2, 3, and 4 are possible sources of attack traffic. One assumption is that a form of PPM is employed by all the routers  $R_{i,j}$  in this graph, where  $i$  is the distance of the router from the victim, and  $j$  is the path linking attacker  $j$  to the victim. Another assumption is that sufficient traffic is generated by Source 1 for the victim to have collected marked packets from all routers  $R_{i,1}$  in the path linking them to Source 1. Given this setup, our approach is to build a graph from the marked packets linking Source 1 to the

victim and use that graph to predict where other packets are coming from. We define *known routers* as the routers that are included in the graph built on legitimate traffic.



**Figure 3.4:** *Single Path, Multiple Attacker (SP/MA)*

The best-case scenario is encountered when the entire attack path is already known. In Figure 3.4, that would be the case if Source 3 were the attacker. The packets received by the victim in this attack would not have any unfamiliar routers or edges embedded in them. In fact, just a single packet showing an edge between the victim and router  $R_{m,j}$  is enough to trace the entire attack path all the way from the victim to the source of the attack. The victim would still have to receive a couple more packets to ascertain that there are no markings from routers  $R_{i,j}$  where  $i > m$  and  $j = 3$ . The algorithm would check more packets to ensure that there were no markings from routers farther away than  $R_{m,j}$  but still on the same path.

The average case scenario is when only a part of the attack path is already known. This is just the case if Source 2 is the attacker. The packets received by the victim during the attack would have a mixture of familiar edges ( $i \leq n$ ) and unfamiliar

edges ( $i > n$ ). In this case, the algorithm searches through the marked packets for any packets linking the known router  $R_{n,2}$  to the unknown attack source  $R_{d,2}$ .

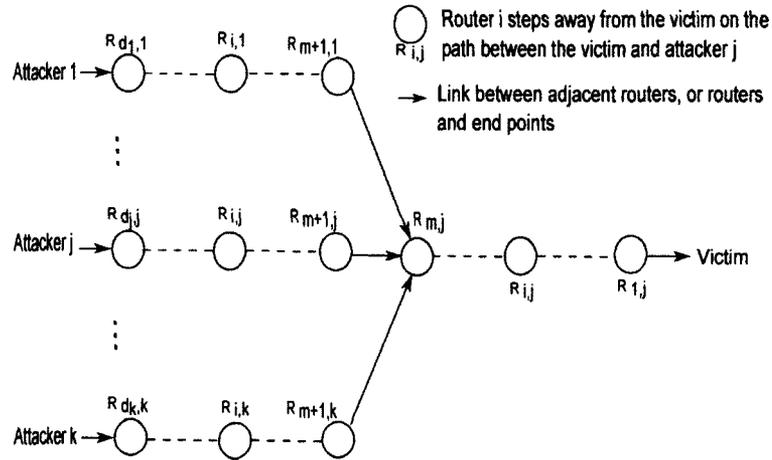
The worst-case scenario is when the entire attack path is unknown. This would be if Source 4 is the attacker. In this case, the packets received by the victim during the attack have unknown edges embedded in them. The algorithm then constructs the attack path using the traditional traceback routine in [38, 49]. No prediction results could be gained by PBS.

### 3.3 Simulation and Results

#### 3.3.1 Simulation Study

To investigate the behavior of the proposed marking scheme, we set up three different network topologies. These are the *Single Path, Single attacker* (SP/SA) in Figure 3.1, *Single Path, Multiple Attacker* (SP/MA) similar to that in Figure 3.4, and the *Multiple Path Multiple Attacker* (MP/MA) in Figure 3.5. These three different scenarios are chosen because we aim to describe any possible attack graph in a network. For example, a DoS attack is similar to the SP/SA topology, while a DDoS attack uses either a SP/MA topology, MP/MA topology, or a combination of all three. To investigate the performance of the traceback algorithm, we additionally consider two larger random networks which we refer to as Topology I, and Topology II.

The topologies and their operations are implemented in NS-2 [35]. Topologies I and II are derived using the *Brite Topology Generator* [32], which was set up to produce NS-2 format output for router level topologies.



**Figure 3.5:** *Multiple Path, Multiple Attacker (MP/MA)*

The SP/SA topology is set up according to Figure 3.1 with the number of attackers  $k = 1$  and the number of nodes  $d_1 = 21$ .

The SP/MA topology is set up according to Figure 3.4 with  $k = 5$ ,  $d_1 = 11$  and distance to common intersection of paths  $m = 4$ .

The MP/MA topology is set up according to Figure 3.5 with  $k = 3$ ,  $d_1 = d_2 = d_3 = 9$ , and  $m = 4$ .

Topology I consists of 50 nodes following the Waxman model [47]. The Waxman model is a random network construction model used to simulate the Internet-like topologies. In this model, nodes are uniformly distributed in a plane, and the probability of an edge being assigned between nodes  $a$  and  $b$ , distance  $d$  apart, is given by the expression  $P(a, b) = \alpha e^{-\frac{d}{\beta L}}$  where  $L$  is the maximum distance between any two nodes [25].

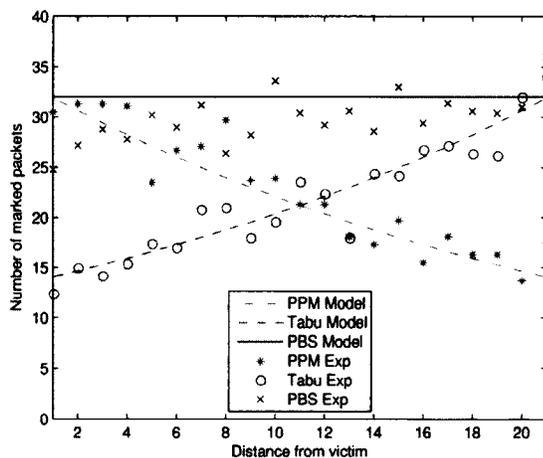
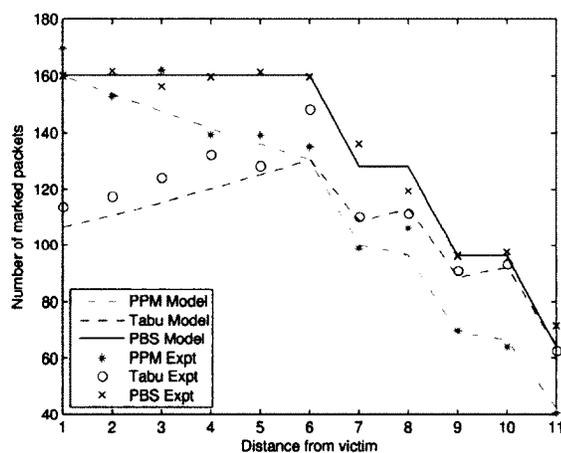
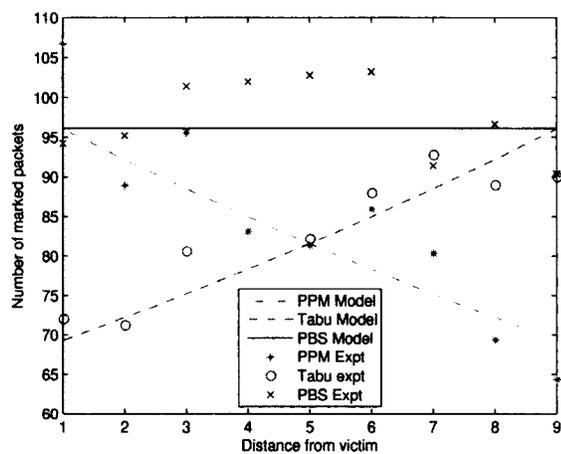
The settings for this model are Waxman components  $\alpha = 0.15$ ,  $\beta = 0.2$ , and the minimum number of links per node being 2.

Topology II consists of 100 nodes with Waxman components  $\alpha = 0.15$ ,  $\beta = 0.2$ , and the minimum number of links per node being 2.

### 3.3.2 Marking Scheme Results

We test the validity of the theoretical models by running simulations for all three marking schemes in the three topologies SP/SA, SP/MA, MP/MA. By plotting the number of marked packets received against the distance from the victim at which they were last marked, Figure 3.6a, Figure 3.6b, and Figure 3.6c show that the experimental results agree with the theoretical models. The figures also show which sections of the attack path produce fewer marked packets. In PPM, the routers more distant from the victim are able to send only half as many packet markings as the routers closer to the victim. For Tabu marking scheme, the routers closer to the victim send fewer packets compared to the routers farther away from the victim. The sections with the fewest packets are the sections that limit the speed with which traceback can be executed with those specific marking schemes.

We evaluate the loss of information in the three schemes over the three topologies. Table 3.1 shows that PPM and Tabu deliver about the same percentage of marked packets as each other regardless of the topology. It also shows that a considerable portion of the packets is marked more than one time when PPM scheme is employed, resulting in loss of information. Both Tabu and PBS avoid information loss due to overwriting, but only PBS compensates by ensuring that more packets in total are marked. In some cases, up to 78% of the packets received are marked in the PBS scheme compared to 57% for Tabu Scheme and 59% for PPM Scheme.

(a) *Single Path, Single Attacker (SP/SA).*(b) *Single Path, Multiple Attacker (SP/MA)*(c) *Multiple Path, Multiple Attacker (MP/MA)*

**Figure 3.6:** Number of marked packets versus distance of last mark for different models. This figure shows how the frequency of router markings in packets received by the victim is dependent on the distance of the router from the victim

**Table 3.1:** Distribution of packets, and the number of times they are marked, in different graphs. SP/SA = Single Path, Single Attacker; SP/MA = Single Path, Multiple Attacker; MP/MA = Multiple Path, Multiple Attacker

Path	Scheme	Number of marked times					Total
		0x	1x	2x	3x	4x	
SP/SA	PPM	40.57	37.88	16.53	4.17	0.75	100%
	Tabu	43.07	56.93	0	0	0	100%
	PBS	21.62	78.38	0	0	0	100%
SP/MA	PPM	68.05	26.54	4.72	0.64	0.04	100%
	Tabu	69.20	30.80	0	0	0	100%
	PBS	63.08	36.92	0	0	0	100%
MP/MA	PPM	68.53	26.21	4.74	0.48	0.04	100%
	Tabu	69.26	30.74	0	0	0	100%
	PBS	63.50	36.50	0	0	0	100%

The average number of marked packets required for traceback in the three topologies for the three marking schemes is shown in Table 3.2. When compared to PPM, PBS only requires 54% of the number of total packets necessary for traceback in the SP/SA scenario, 62% in SP/MA, and 66% in MP/MA.

**Table 3.2:** Average number of total packets required for traceback in different graphs

Path	PPM	Tabu	PBS
Single Path, Single Attacker	188.74	157.94	102.78
Single Path, Multiple Attacker	435.36	304.91	269.78
Multiple Path, Multiple Attacker	398.60	309.64	261.84

Even though PBS and Tabu both do not overwrite marked packets, PBS performs superior to Tabu because it writes the information in the next available packet. Our approach is therefore able to achieve faster convergence with just one extra bit, in terms of space, required at the routers.

### 3.3.3 Traceback Scheme Results

To investigate the traceback scheme, we consider two additional topologies designed to resemble the Internet in terms of connectivity. All five topologies are used to compare the traditional traceback algorithm to the PBS traceback algorithm. The results are given in Table 3.3. To ensure that the comparison among the different schemes is due to the distribution of marked packets and not influenced by the increased number of marked packets in PBS compared to PPM and Tabu, we only consider the number of *marked* packets that are necessary for traceback.

**Table 3.3:** Average number of marked packets required for traceback in different graphs (Traditional traceback / Our traceback scheme)

Path	PPM	Tabu	PBS
Single Path, Single Attacker	42/42	39/21	47/44
Single Path, Multiple Attacker	29/29	10/2	16/10
Multiple Path, Multiple Attacker	12/4	12/12	10/7
Topology I	11/8.8	5/1.6	3/1.6
Topology II	15/14.1	11/11	5/4.6

For the SP/MA and MP/MA topologies, all but one of the sources of traffic are categorized as legitimate and the one remaining categorized as attack traffic. Using the graphs built from the legitimate traffic sources, the PBS traceback algorithm is able to decrease the number of marked packets necessary for traceback down to 20% for Tabu and 33% for PPM.

The SP/SA topology legitimate graph is set up by introducing a legitimate source located in the middle of the attack graph. In that scenario, the PBS traceback

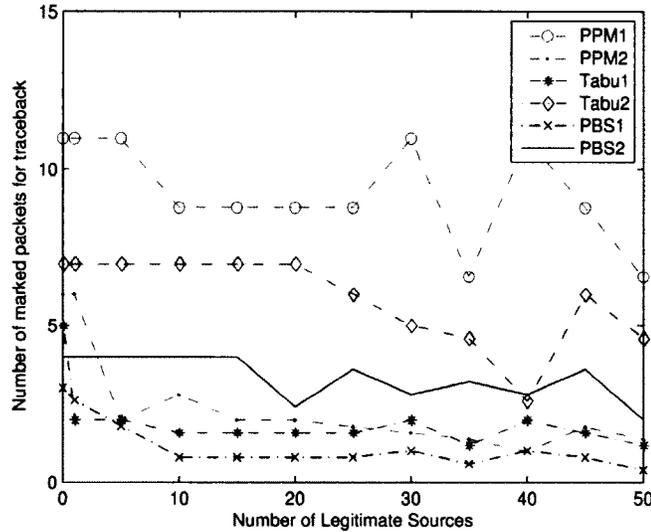
algorithm is able to cut down on the number of packets necessary for traceback down to 54% in Tabu.

Topology I is made up of 50 nodes with four randomly chosen sources of traffic. Because of the high level of connectivity, the average path length between any two random nodes is about 3.5 hops. Three of the four sources are categorized as legitimate traffic and the graph built from their packets is used to predict where the fourth randomly chosen source of packets (attacker) is located. The prediction extension to the traceback scheme was able to cut the number of marked packets required for traceback down to 32% in Tabu, 53% in PBS, and 80% in PPM.

Topology II is made up of 100 nodes with ten randomly chosen sources of traffic. The average path length between any two randomly selected nodes is only about 4-5 hops. Eight of the ten sources are categorized as legitimate and used to build a graph to predict the origin of the packets from the remaining two sources (attackers). Because of the low possibility of common paths in such a large and connected network, the prediction component only yields marginal improvement.

We also investigate the effect of increasing the number of legitimate sources on the number of marked packets required for complete attack graph construction. This is done by randomly selecting nodes from Topology II and using traffic from those nodes to build a legitimate graphs. The traceback algorithm is then run to trace randomly selected attack nodes for different sizes of legitimate graphs. This is done for the simplified scenarios of one and two attackers. As shown in Figure 3.7, the number of marked packets required to trace the attackers is generally lower for larger

legitimate source graphs. The outliers are attributed to the worst case scenario when the legitimate graphs and attack graphs do not share any common edges.



**Figure 3.7:** Effect of increasing number of legitimate sources on the number of marked packets required for traceback of one attacker (PPM1, Tabu1, PBS1) and two attackers (PPM2, Tabu2, PBS2)

### 3.4 Conclusions

In this chapter, we have presented two enhancements to the PPM traceback schemes. First, we present a novel marking scheme that allows a complete traceback with a minimized number of received packets. Secondly, we extend an existing traceback algorithm by a prediction component.

The proposed marking scheme ensures that packet markings from different sections of the attack path have the same chance of arriving at the victim. This results in the attack path being constructed with almost half as many received packets as previous schemes.

A traceback algorithm has been extended by a prediction component, which builds graphs based on legitimate traffic collected prior to or after an attack. A feature of this extended traceback algorithm is to predict the attack packets' paths without receiving markings from all routers in the path.

Results show that the marking scheme makes it possible for complete graph construction with 54% of the total packets required with traditional techniques. The prediction component in the traceback algorithm also allows for complete traceback to be possible with 33% of the usual number of marked packets.

Both techniques presented in this paper can be used independently to improve existing PPM-based techniques.

## CHAPTER 4

# NETWORK DEPENDENCY OF PPM-BASED SCHEMES

### 4.1 Problem Statement

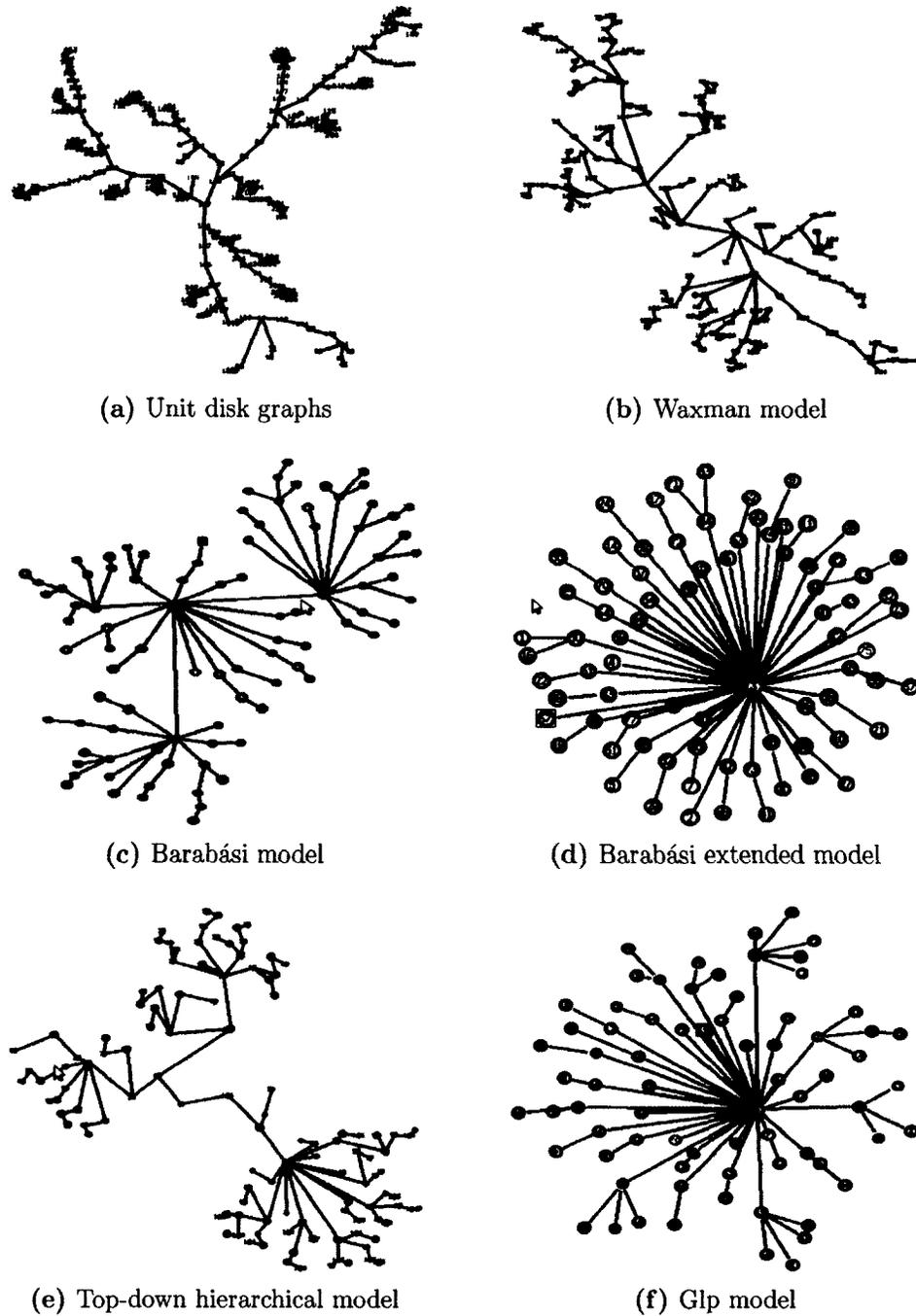
Whereas network protocols such as PPM-based schemes are designed and assumed to be independent of the underlying network topology, the topology sometimes has a large influence on protocol performance [38, 41]. As a result, researchers typically evaluate network related protocols on the exact network topology for which they are designed. Such evaluations enable the researchers to identify topology properties that could affect the protocol's performance. These evaluations provide insights that can either be leveraged to yield better protocol performance, or can provide an indication of what problems may be faced during the protocol deployment.

However, because carrying out experiments on the Internet itself is expensive and inflexible, researchers resort to simulations using *Internet-like topologies*. Internet-like topologies refer to network topologies that demonstrate the characteristics exhibited in the Internet and are created using mathematical models that have been shown to describe the nature of the Internet topological structure [41]. In this paper, we study the impact of network topology on PPM-based schemes by considering a set of 60 distinct networks selected to encompass the variety of models in the field of Internet modeling.

Figure 4.1 shows six sample attack graphs derived from six different models of networks. These models include the unit disk graphs, the Waxman model, two Barabási models, the hierarchical model, and the *generalized linear preferential* (GLP) model [16, 47, 4, 56, 32, 13, 12]. Each attack graph is derived from a DDoS attack of the same scale simulated on networks of equal size. Despite the similarity in both network size and attack scale, the attack graphs are different in both size and structure and consequently in convergence time. These attack graphs show how traceback results can be very different from one network to another. Our work presents the first step in understanding why these attack graphs are so different.

In this paper, we discuss three network-dependent factors that affect PPM-based scheme performance. We show how these factors lead to differing convergence times among the different schemes. We then provide a comparative study of three schemes in the aforementioned set of 60 networks. To capture similarities and differences within the set of considered networks, we adapt the *network motif* approach to Internet-like networks [34, 33, 28]. We use this approach to categorize networks of different models and origins into *superfamilies* according to their basic structure.

This study can be used to provide more accurate predictions for both the performance of PPM-based schemes in attack graph reconstruction, and the structure of attack graphs in any Internet-like network.



**Figure 4.1:** Sample attack graphs from networks built using the described network models. The attack graphs consist of 50 attackers and the paths that the traffic they generate takes to get to the victim node (marked in red). Given that the overall topologies are of the same size, these figures show significant differences in the general structure of attack graphs, which in turn depends on the underlying model used to construct the network topologies

In the following section, we show specific attack graph scenarios designed to illustrate the identified network-dependent factors. In Section 4.3, we show how network motifs are identified and how *subgraph ratio profiles* (SRPs) are derived from the considered networks. We also show how the derived SRPs are used to identify superfamilies within the networks.

## 4.2 Approach

In this work, we evaluate and compare the performance of three PPM-based schemes (PPM [38], TMS [30], PBS [26]) on the set of networks. This allows us to identify network based factors that affect the schemes' performances in the different networks. The identified factors include the average path length, the overlapping of attack paths, and the occurrence of network motifs in attack graphs. In the subsequent subsections, we describe how each of these factors has a unique effect on the schemes' convergence times for DDoS attack graphs.

Previous analytical modeling of the convergence time of PPM-based schemes captures its dependence on the marking probability  $p$  and the attack path length  $d$ . By using the *coupon collector problem*, Savage *et al.* [38] show that the expected convergence time of an attack path is bounded by the expression  $E[x] \leq \frac{\ln(d)}{p(1-p)^{d-1}}$ . In this expression, the limiting term  $p(1-p)^{d-1}$  represents the probability of receiving a marking from the *least likely edge*. The least likely edge refers to the edge in the attack graph whose markings are received with the least frequency by the victim. The above expression shows that the convergence time decreases with an increase in the frequency of the least likely edge, and vice versa. The location and probability of

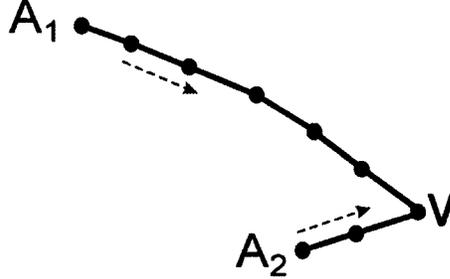
the least likely edge varies with the marking scheme that is employed in the attack graph. We use this model to explain the impact of the network factors on the schemes' convergence times.

#### 4.2.1 Average Path Length

According to the model proposed by Savage *et al.* [38], one of the factors that affects convergence time is attack path length. However, during the evaluation of a scheme in a large scale network, the specific attack path lengths for all the attackers are not easily accessible. In this case, the average shortest path length can be used as an indicator of how long a typical attack path would be in that network, but this has its shortcomings in terms of the accuracy of convergence time prediction. As we show later on, this is because it is possible to have two attack graphs of identical average attack path length, but different attack path lengths, and therefore different convergence times.

Consider Figure 4.2 which shows an attack graph linking attackers  $A_1$  and  $A_2$  to victim  $V$ .  $A_1$  and  $A_2$  are located six and two hops from the victim, respectively, and their attack paths do not overlap. This attack graph exhibits an average path length of four hops. Contrast this attack graph with one where both  $A_1$  and  $A_2$  are located four hops from the victim. In the new set up, the average attack path length is unchanged, but the specific attack path lengths, and consequently their convergence times, have been changed. We use this set up to investigate how different attack graphs affect the convergence times for different schemes. The attack path lengths are

varied while ensuring that the average attack path length is kept constant in every set up.



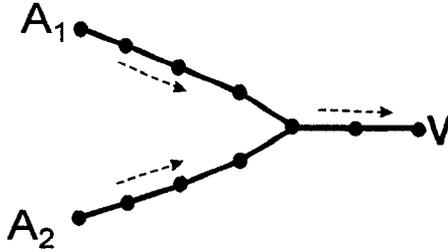
**Figure 4.2:** 2-attacker V-shaped attack graph with different path lengths. Attacker  $A_1$  is two hops away from the victim  $V$  while attacker  $A_2$  is six hops away from the victim. Different attack path lengths have a considerable effect on the convergence time of the attack graph

#### 4.2.2 Overlapping of Attack Paths

The original analytical model for convergence time presented by Savage *et al.* [38] assumed independent attack paths. When one considers a more connected underlying topology, attack paths from different attackers are likely to merge close to the victim. The merging of attack paths yields a tree-like attack graph. An attack graph with overlapping attack paths has fewer unique edges than a similar size attack graph with no overlapping edges. Since there are fewer edges to identify, overlapping attack paths translate to reduced convergence times for PPM-based schemes.

While there is a general reduction in convergence time with overlapping of attack paths, the manner of this reduction varies with the marking scheme being employed. Consider Figure 4.3 which shows two attack paths from attackers  $A_1$  and  $A_2$  to victim  $V$  that overlap for two hops. Recall that the expected convergence time is limited by the *least likely edge*. In the case of PPM, the least likely edge is located

closest to the attacker. Because the overlap of the attack paths is closer to the victim, the overlap does not affect the probability of the least likely edge. Therefore, the reduction in convergence time associated with any increase in the amount of overlap is purely due to the lower number of edges to identify in the attack graph.



**Figure 4.3:** 2-attacker Y-shaped attack graph with overlapping attack paths. Attackers  $A_1$  and  $A_2$  are both six hops from the victim  $V$ , but the attack paths share an overlapping section of two hops. The amount of overlap between different attack paths has a big effect on the convergence time of the attack graph

Contrast this with TMS where the least likely edge is typically located closer to the victim. When attack paths merge, as in Figure 4.3, the edges closer to the victim experience an increase in their probability since there is increased traffic flowing through them compared to other parts of the attack path. The increased traffic flowing through the edges closer to the victim comes from all the attack paths that have merged by that point. An increase in the probability of the *least likely edge* translates to lower convergence times. We therefore should expect to see a sharper decline in convergence times in TMS than in PPM.

The analysis for PPM applies to all other PPM-based schemes where the least likely edge is located closest to the attacker [39, 49, 23]. The merging and overlap of attack paths does not affect the probability of these edges; therefore, the reduction in convergence time is due to a reduction in the size of the attack graph. On the other

hand, the analysis for TMS applies to other PPM-based schemes where the least likely edge is located closest to the victim such as PBS [44, 26].

We investigate the influence of the amount of overlap of two attack paths on the convergence time of the entire attack graph by using a set up similar to Figure 4.3. To do this, we vary the amount of overlap and observe how the convergence times for different schemes change.

### 4.2.3 Occurrence of Motifs in Attack Graphs

Previous modeling and analysis of PPM-based schemes has typically assumed that an attack graph is tree-structured with the victim located at the root node, and the attackers located at the leaf nodes [38, 49, 30, 44, 26, 23]. Tree-structured attack graphs exhibit a single path from any given attack node to the victim node. This assumption is based on the observation that typical Internet traffic paths are largely constant, especially over short periods of time [37]. However, the flooding that is associated with a DDoS attack could lead to uncommon traffic patterns. An example of such a pattern is traffic being forwarded along alternative paths in order to deal with congestion [3, 43]. This factor should be considered when the simulations are carried out on Internet-like networks.

The motifs of a network can be used to provide an indication of the kind of alternative paths that can be expected to appear in attack graphs from that network. Because network motifs represent the specific subgraphs that are prevalent in a network, there is a considerable chance that attack graphs derived from that network will also exhibit those specific subgraphs. However, only four of the six 4-node subgraphs shown



### 4.3 Network Classification Using Motifs and Subgraphs

Comparing large-scale networks to find similarities and differences is a complicated problem. This is because networks can be described using a variety of attributes, the majority of which are not easy to obtain. Additionally, the set of attributes that describe one type of network is often different from the set of attributes that describe another type of network. This becomes even more complicated when one compares naturally occurring networks whose formation has no simple mathematical formulation or modeling.

The methodology of network motifs and subgraphs solves this comparison problem by comparing networks using subtle structural differences while ignoring their construction principles and other network specific attributes. The advantage of this method is that it can be easily applied to networks from all fields and can therefore be used to identify similarities between networks that would traditionally be difficult to compare.

#### 4.3.1 Motifs and SRPs

The six possible undirected 4-node subgraphs found in a network topology are shown in Figure 4.4. Every undirected large-scale network will exhibit at least one of these subgraphs regardless of their construction principles or attribute settings [34, 33]. The motif and subgraph method uses the relative presence or absence of these subgraphs to differentiate the networks.

The *subgraph ratio profile* (SRP) of any given network is a plot describing the relative abundance or scarcity of the six 4-node subgraphs in that network. This

plot is obtained by counting the number of times that the subgraphs appear in a given test network, and comparing this value with the average number of times the same subgraphs appear in randomized networks of the same size and connectivity. This comparison enables us to identify the subgraphs that are statistically significant compared to similar random networks. For each subgraph  $i$ , a relative score  $R_i$  is calculated from  $R_i = \frac{N_{test,i} - \bar{N}_{rand,i}}{N_{test,i} + N_{rand,i} + \varepsilon}$  [33], where  $N_{test,i}$  is the number of times subgraph  $i$  appears in the test network, while  $\bar{N}_{rand,i}$  is the average number of times it appears in the similar randomized networks. As in [33],  $\varepsilon$  is set to 4 to ensure that large  $R_i$  values are not obtained with relatively low  $N_{test,i}$  and  $\bar{N}_{rand,i}$  values.

All six  $R_i$  values for the test network (corresponding to the six 4-node undirected subgraphs) are then normalized using the expression  $SRP_i = \frac{R_i}{\sqrt{\sum_{i=1}^6 R_i^2}}$  [33] to yield a six value SRP vector that uniquely describes that network. Positive  $SRP_i$  values suggest an abundance of subgraph  $i$  in the network, while negative values suggest the contrary.

A subgraph is referred to as a *network motif* if it is significantly prevalent in the test network when compared with the randomized networks [34]. We use the  $Z$ -score  $Z_i$  of any of subgraph  $i$  to quantify its level of prevalence. The  $Z$ -score is evaluated using  $Z_i = \frac{N_{test,i} - \bar{N}_{rand,i}}{\sigma_{rand,i}}$  [34] given  $\sigma_{rand,i}$  is the standard deviation of subgraph  $i$ 's occurrence frequency in the randomized networks. Therefore, a subgraph  $i$  is referred to as a network motif if  $Z_i \geq 3.0$  [34].

### 4.3.2 Identifying Network Superfamilies

Using the network SRPs, the networks can be grouped according to their similarity. Similar to the cluster selection problem in data mining, identifying the number of superfamilies from a set of networks is subjective and can be ambiguous. Combined with a  $k$ -nearest neighbor algorithm, a correlation map of the network SRPs can be used to provide a rough idea of how many superfamilies a set of networks contains. Such a map would show the level of similarity exhibited between different networks and within possible superfamilies.

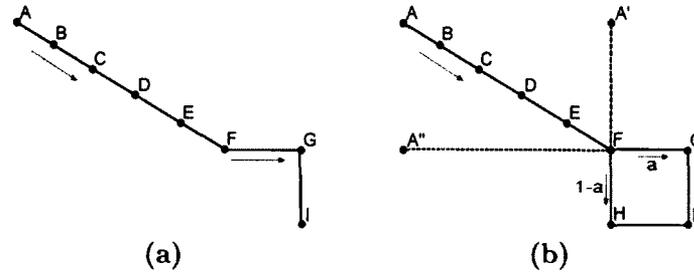
A  $k$ -means clustering algorithm can then be used to find a more accurate number of clusters from the SRPs. By running this algorithm for different numbers of clusters  $m$ , and recording the intra-cluster error  $e(m)$ , one is able to identify an appropriate cluster number  $k$  using the expression  $k = \min\{m | m \in [2, n] \cap \frac{e(m+1)-e(m)}{e(m)} \leq t\}$ , where we set the limiting error  $t = 10\%$ . The number of clusters is appropriate because it represents a trade off between accuracy and cluster size. Each network is assigned to a cluster which then constitutes a superfamily.

## CHAPTER 5

### SYSTEM MODEL AND ANALYSIS

In this chapter, we propose an analytical model which shows how subtle differences in network topologies contribute to differences among the convergence times of the PPM-based schemes. The structural differences contribute to two factors, namely *alternative paths* and *merging of attack streams*. These factors affect each scheme uniquely and yet their level of influence varies depending on the network topology. As a result, the performance of different schemes will be similar in one network, and yet dissimilar in another network.

To illustrate these factors, we refer to Figure 5.1, which shows an attack stream taking a path from Node A to the victim at Node I. In Figure 5.1a, the attack stream takes a single route to the victim. In Figure 5.1b, the attack stream from Node A takes two routes to get to the victim. By definition, an attack stream could consist of network packets from any number of upstream sources, as long as the packets are being forwarded along the same path to the same destination. However, for simplicity, we consider the stream from Node A as having originated at a single attacker located at A.



**Figure 5.1:** Sample attack paths linking attacker A to victim I. The attack path in Figure b exhibits Subgraph 4 in which the traffic can either take path FGI with probability  $a$ , or path FHI with probability  $1 - a$

### 5.1 Traditional Analytical Model

Originally, the convergence time for PPM-based schemes has been modeled as the *coupon-collector's problem* [21, 38]. In the classic problem, a coupon collector seeks to collect  $d$  equally likely distinct coupons by drawing them from an urn with replacement. While it takes a short time to get the first few unique coupons, it takes considerably longer to get the last few coupons that complete the entire collection. The expected number of turns needed to draw all  $d$  distinct coupons grows as  $\Theta(d \cdot \ln(d))$  [21].

When the coupon collector problem is applied to packet marking, the marked packets are taken to be the coupons. For example, Figure 5.1a shows a single path linking attacker A to victim I and the target of the “coupon collector” would be to collect markings for all seven edges. However, the expected time expression above cannot be directly applied to the packet marking problem for two reasons. Firstly, while one is guaranteed to pick a coupon with each draw in the coupon collector problem, one may or may not “draw” a marked packet in the packet marking problem. This is because a sizable proportion of the packets received by the victim do not

contain any router information because they were not selected to be marked by any of the routers in their path to the victim. Secondly, while the coupons in the classic problem have equal chances of being drawn, the marked packets have unequal chances of being received. Savage *et al.* [38] deal with the unequal edge probabilities by utilizing the probability of the *least likely edge* to provide an upper bound on the expected convergence time.

Formally, given a single path of  $l$  hops implementing the PPM scheme with router marking probability  $p$ , the *least likely edge* is typically the edge located closest to the attacker which has a probability  $p(1 - p)^{l-1}$  of being received by the victim. Given  $d$  unique markings, the probability of receiving any marking at the victim is therefore at least  $dp(1 - p)^{l-1}$ , which is the product of the number of unique markings and the probability of the *least likely edge*. The expected number of packets  $E[x]$  required to complete the marking “collection” in order to build the attack graph is derived by dividing the original coupon collector expectation by  $dp(1 - p)^{l-1}$ , which yields Equation 5.1 [38]:

$$E_{0,PPM}[x] < \frac{\ln(d)}{p(1 - p)^{l-1}}. \quad (5.1)$$

Therefore, the traditional expression for the upper bound of the expected convergence time is obtained by dividing the natural logarithm of the number of distinct edges  $d$ , by the probability  $p(1 - p)^{l-1}$  of the *least likely edge* in the attack path. For the SP/SA topology, the number of hops is equal to the number of unique markings ( $l = d$ ).

Similarly, the convergence time expressions for TMS and PBS are given by Equations 5.2 and 5.3, respectively. In these expressions, the probability of the *least likely edge* in an SP/SA is given by  $p(1-p)^{l-1}$  for TMS and  $p$  for PBS. In contrast to PPM, the least likely edge for TMS and PBS is the edge located closest to the victim<sup>1</sup>:

$$E_{0,TMS}[x] < \frac{\ln(d)}{p(1-p)^{l-1}}, \quad (5.2)$$

$$E_{0,PBS}[x] < \frac{\ln(d)}{p}. \quad (5.3)$$

## 5.2 The Effect of Motifs on the Analytical Model

One hitherto unstudied factor that affects the convergence time is the alternative paths that traffic might take. To understand the influence of the *alternative paths* factor, we consider an attack graph containing a subgraph which exhibits alternative paths. Figure 5.1b shows such an attack graph linking attacker A to victim I in which the attack traffic takes one of two paths FGI or FHI with probability  $a$  and  $1-a$ , respectively. The nodes F, G, H and I in this attack graph form Subgraph 4. While the attack path length  $l$  is unchanged (from Figure 5.1a to Figure 5.1b), the probability and the location of the least likely edge is considerably altered and, consequently, the convergence time is changed.

The alternative path factor  $a$  is affected by a variety of factors such as the presence of load balancing routers in the network, the number of alternative paths available, the amount of traffic being processed at Node F, as well as the bandwidth and latency values for the alternative paths. For the analysis in this section, we

---

<sup>1</sup>While PBS typically exhibits equal probability for all edges in the attack path, the *saturation condition* potentially makes probabilities of edges closer to the victim less likely than the rest. This condition occurs for either long path lengths, or high marking probabilities.

assume node F has load balancing capability, and the routes can sustain the traffic being forwarded through them.

Consider the case of PPM. In Figure 5.1a, the least likely edge is AB with a probability of  $p(1-p)^{l-1}$ . However, the probability of receiving edge FG in Figure 5.1b is given by  $ap(1-p)$ , which is considerably less than the probability of AB for short path lengths<sup>2</sup>. This means that the least likely edge and its corresponding probability have changed and Equation 5.1 has to be altered accordingly. In this case, the convergence time is given by Equation 5.4:

$$E_{1,PPM}[x] < \frac{\ln(d)}{ap(1-p)}. \quad (5.4)$$

Comparing Equation 5.1 and Equation 5.4 reveals that the convergence time is increased by a factor of  $\frac{(1-p)^{l-2}}{a}$ . This means that even in the best case when both alternative paths are equally likely ( $a = 0.5$ ), the convergence time of a 3-hop attack graph is multiplied by a factor of 1.92 while a 15 hop attack graph is multiplied by a factor of 1.18. If one of the two paths only carries a tenth of the traffic ( $a = 0.1$ ), the convergence times of the 3-hop and 15-hop attack graphs is multiplied by a factor of 9.6 and 5.88, respectively. This shows that, for PPM, the alternative paths factor affects short attack paths more than long attack paths.

Consider the case of TMS. The least likely edge in Figure 5.1a would be GI with a probability of  $p(1-p)^{l-1}$ . When alternative paths are considered in Figure 5.1b, the probability of GI is reduced even further to  $ap(1-p)^{l-1}$ , which means the

---

<sup>2</sup>In this scenario, a short path is any path less than 18 hops long. This is evaluated from  $\{p(1-p)^{l-1} < ap(1-p) \iff l > 18\}$ . The limit of  $l$  is evaluated for equal chance of taking either route ( $a = 0.5$ ) and a marking probability  $p = 0.04$ .

convergence time is given by Equation 5.5:

$$E_{1,TMS}[x] < \frac{\ln(d)}{ap(1-p)^{l-1}}. \quad (5.5)$$

Comparing Equation 5.2 and Equation 5.5 shows that the convergence time is increased by a factor of  $\frac{1}{a}$  regardless of the path's length. This means that if both alternative paths are equally likely ( $a = 0.5$ ), the convergence time is doubled, and if one path only takes a tenth of the traffic ( $a = 0.1$ ), then the convergence time is increased by a factor of 10.

The PBS case is very similar to the TMS case. The least likely edge in Figure 5.1b is GI and its probability changes from  $p$  to  $ap$  when one considers the alternative paths. Consequently, the convergence time changes to Equation 5.6:

$$E_{1,PBS}[x] < \frac{\ln(d)}{ap}. \quad (5.6)$$

Comparing Equation 5.3 and Equation 5.6 shows that the convergence time is increased by a factor of  $\frac{1}{a}$  regardless of the path's length which, is similar to the TMS case.

This shows that alternative paths reduce the probability of the least likely edges in an attack path for all the considered schemes, and consequently increases their convergence times. However, their impact on convergence times is higher in TMS and PBS than it is in PPM.

### 5.3 The Effect of Path Merging on the Analytical Model

Another factor that comes into play in the convergence time is the *merging of attack streams* as different attack paths get closer to the victim [49]. As a result of

this merging, the probabilities of downstream edges in an attack path are increased which affects its convergence time. To understand the influence of merging, consider the attack graph in Figure 5.1b where two other attack streams from attackers A' and A'' contribute an equivalent amount to the traffic flowing out of Node F towards Victim I. Because of the increased traffic flowing through edges FG, FH, GI, and HI, there is an increased chance of receiving markings from those edges, which in turn affects the reconstruction time of the attack path of attacker A.

Consider the PPM case. With just attacker A and short attack paths, we showed that the least likely edge is FG with a probability of  $ap(1 - p)$  and the convergence time is given by Equation 5.4. However, with attackers A' and A'', the traffic going through FG is 3 times as high and so is the probability of receiving its marking. Formally, given  $n$  equivalent attack streams merging before node F, the probability of receiving FG changes to  $nap(1 - p)$ . This means that when  $na \geq 1$ , edge FG is no longer the least likely edge in the attack path from attacker A. In this case, the least likely edge reverts to edge AB whose probability is still  $p(1 - p)^{l-1}$  and consequently the convergence time expression reverts to Equation 5.1. This means that the merging of attack streams has the potential to offset the alternative paths factor for PPM.

Consider the TMS case. With attacker A, we showed that the alternative paths reduced the probability of edge GI to  $ap(1 - p)^{l-1}$ . The increased traffic from A' and A'' increases this value to  $nap(1 - p)^{l-1}$ , which in turn nullifies the influence of the alternative paths when  $na = 1$ . However, when  $na > 1$ , edge GI ceases to be the least likely edge. In this condition, the least likely edge is the edge closest to the victim

whose traffic and probability are unaffected by the merging attack streams. In Figure 5.1b, this happens to be edge EF. The probability of receiving edge EF is  $p(1-p)^{l-3}$ , which means the convergence time changes from Equation 5.5 to Equation 5.7:

$$E_{2,TMS}[x] < \frac{\ln(d)}{p(1-p)^{l-3}}. \quad (5.7)$$

Comparing 5.2 and Equation 5.7 shows that the merging of attack streams not only nullifies the alternative path's factor, but also reduces the convergence time. The amount by which the convergence time is reduced depends on how close the "new" least likely edge is to the attacker. The closer the new least likely edge is to the attacker, the more the reduction in convergence time, and vice versa. In this particular scenario, the new least likely edge (EF) is two positions away from its original position (GI), and the convergence time reduces to  $(1-p)^2$  of its original value. Given  $p = 0.04$ , the convergence time is reduced by 8% of its original value.

Analysis of the PBS scheme yields insights similar to those gained from the analysis of the TMS scheme. Given a similar scenario, the probability of receiving edge GI increases from  $ap$  to  $nap$ . As with the TMS scheme, the merging of the attack streams not only cancels out the alternative path effect but reduces the expected convergence time as well.

This shows that the merging of attack streams offsets the alternative path effect for all the considered schemes. However, while the merging simply cancels out the alternative path effect in PPM, it reduces the convergence time for TMS and PBS.

The model presented thus far considers subgraph 4, which exhibits two alternative paths. Table 5.1 shows the probabilities for the least likely edges for

subgraphs 3, 4, 5 and 6 under various traffic conditions. The probabilities in the “Original” column show the expressions when both alternative paths and merging of attack streams are ignored. The probabilities under the “Number of merging streams” column show these same probabilities when one considers the given subgraphs with a different number of merging attack streams. As in Figure 5.1b, we consider an attack graph where the different attack streams merge at the node just before the subgraph. Additionally, the victim node is part of the subgraph and the probability of taking any of the alternative paths is equal. While this set up is specific, the analysis obtained from it can be used to describe the influence of both alternative paths and merging attack streams in a larger network. The probabilities in the table reveal that it takes more merging attack streams to offset the alternative paths in subgraphs 5 and 6 than in subgraphs 3 and 4. This is because subgraphs 5 and 6 exhibit more alternative paths and consequently require more attack traffic to offset the drop in probability caused by the alternative paths. For example, with two merging streams in subgraph 4 and PPM, the probability of the least likely edge is  $p(1 - p)^{l-1}$ , which is the same as the original probability. However, with subgraph 6 the probability of the least likely edge under the same conditions is  $2ap(1 - p)$ . In fact, it takes four attack streams to increase that probability back to  $p(1 - p)^{l-1}$ . A higher probability for the least likely edge translates to a lower value for the convergence time, and a lower probability for the least likely edge translates to a higher convergence time.

**Table 5.1:** The table shows 4-node subgraphs and the probabilities of the *least likely edge* for the different marking schemes for  $n$  merging attack streams, along side the original probability of the *least likely edge* given no subgraphs or convergence. The marking probability is denoted by  $p$ , the path length by  $l$ , the probability of taking alternative routes denoted by  $a, b, c$ , with the expressions for PPM, TMS, and PBS shown. For simplicity, it is assumed the probability of taking alternative routes is equal. The convergence time of the marking scheme is indirectly proportional to the lowest probability

IDs	Subgraphs	Scheme	Original	Number of merging streams				
				$n = 1$	$n = 2$	$n = 3$	$n = 4$	$n = 5$
3		PPM	$p(1-p)^{(l-1)}$	$ap(1-p)$	$\geq p(1-p)^{(l-1)}$	$\geq p(1-p)^{(l-1)}$	$\geq p(1-p)^{(l-1)}$	$\geq p(1-p)^{(l-1)}$
		TMS	$p(1-p)^{(l-1)}$	$ap(1-p)^l$	$p(1-p)^l$	$p(1-p)^{(l-2)}$	$p(1-p)^{(l-2)}$	$p(1-p)^{(l-2)}$
		PBS	$p$	$ap$	$p$	$p$	$p$	$p$
4		PPM	$p(1-p)^{(l-1)}$	$ap(1-p)$	$p(1-p)^{(l-1)}$	$p(1-p)^{(l-1)}$	$p(1-p)^{(l-1)}$	$p(1-p)^{(l-1)}$
		TMS	$p(1-p)^{(l-1)}$	$ap(1-p)^{(l-1)}$	$p(1-p)^{(l-1)}$	$p(1-p)^{(l-3)}$	$p(1-p)^{(l-3)}$	$p(1-p)^{(l-3)}$
		PBS	$p$	$ap$	$p$	$p$	$p$	$p$
5		PPM	$p(1-p)^{(l-1)}$	$ap(1-p)$	$2ap(1-p)$	$\geq p(1-p)^{(l-1)}$	$\geq p(1-p)^{(l-1)}$	$\geq p(1-p)^{(l-1)}$
		TMS	$p(1-p)^{(l-1)}$	$ap(1-p)^l$	$2ap(1-p)^l$	$p(1-p)^l$	$p(1-p)^{(l-2)}$	$p(1-p)^{(l-2)}$
		PBS	$p$	$ap$	$2ap$	$p$	$p$	$p$
6		PPM	$p(1-p)^{(l-1)}$	$ap(1-p)$	$2ap(1-p)$	$3ap(1-p)$	$\geq p(1-p)^{(l-1)}$	$\geq p(1-p)^{(l-1)}$
		TMS	$p(1-p)^{(l-1)}$	$ap(1-p)^l$	$2ap(1-p)^l$	$3ap(1-p)^l$	$p(1-p)^l$	$p(1-p)^{(l-2)}$
		PBS	$p$	$ap$	$2ap$	$3ap$	$p$	$p$

In summary, the model and analysis presented here shows that *alternative routes* reduce the probability of specific edges in the attack graph and, as a result, increase the convergence time for those attack graphs particularly for TMS, PBS and short attack paths implementing PPM. The *merging of attack streams* offsets this effect in PPM, TMS and PBS. However in TMS and PBS, the merging has the added effect of reducing their convergence times.

## CHAPTER 6

### SIMULATION STUDY

Table 6.1 shows the 60 networks that are considered in this study, some of their properties, and the superfamilies to which they were assigned. These properties include the setup properties, such as the underlying model, and appropriate settings required to build each specific network. Additionally, network specific properties, e.g. average shortest path length and network motif IDs, are shown. Each of the networks consists of 1000 nodes representing routers in a network, all of which employ the marking schemes. One of the nodes is selected to be the victim and 50 other nodes are randomly selected to be the attackers. Using NS-2 [35] as our simulation environment, traffic is sent from the attackers to the victim, and the convergence time for the entire attack graph is measured in packets. This simulation is carried out 200 times for each network and each marking scheme to give a more accurate representation of the network's performance in IP traceback.

**Table 6.1:** Topologies considered, their underlying model, setup settings, average *shortest path length* (SPL) in hops, the *network motifs* (M-ID) identified in those networks, and their assigned *superfamilies* (SF)

Model	Name	Settings	SPL	M-ID	SF
Barabási ( $e, d_{max}, m$ )	Bar01	999,44,1	7.05	—	3
	Bar02	1997,69,2	4.13	—	3
	Bar03	2994,102,3	3.50	—	3
	Bar04	3990,140,4	3.13	—	5
	Bar05	4985,109,5	2.96	6	5
	Bar06	999,58,1	6.70	—	3
	Bar07	1997,67,2	4.09	—	3
	Bar08	2994,103,3	3.49	—	3
	Bar09	3990,135,4	3.14	—	5
	Bar10	4985,93,5	2.98	6	5
Barabási ext. ( $e, d_{max}, p, q, m$ )	Bar11	2048,35,0.25,0.5,1	4.11	3,4,5	1
	Bar12	4077,52,0.25,0.5,2	3.37	3,5	1
	Bar13	6411,384,0.25,0.5,3	2.82	3,5,6	1
	Bar14	7886,323,0.25,0.5,4	2.70	—	5
	Bar15	9800,396,0.25,0.5,5	2.56	5,6	1
	Bar16	2060,31,0.25,0.5,1	4.16	4	1
	Bar17	3941,327,0.25,0.5,2	3.10	—	5
	Bar18	6030,286,0.25,0.5,3	2.93	5,6	1
	Bar19	7742,351,0.25,0.5,4	2.71	—	5
	Bar20	10230,370,0.25,0.5,5	2.54	—	5
Top-down ( $e, d_{max}, u, d$ )	Tdn01	2001,19,2,500	7.82	3,4,5	4
	Tdn02	2005,16,4,250	8.09	3,4,5	4
	Tdn03	2007,17,5,200	9.03	3,4,5	4
	Tdn04	2015,15,8,125	9.69	3,4,5	4
	Tdn05	2020,15,10,100	9.40	3,4,5	4
	Tdn06	2001,17,2,500	7.03	3,4,5	4
	Tdn07	2004,19,4,250	8.44	3,4,5	4
	Tdn08	2007,17,5,200	8.44	3,4,5	4
	Tdn09	2016,15,8,125	9.24	3,4,5	4
	Tdn10	2020,15,10,100	10.42	3,4,5	4

Table 6.1 (continued)

Model	Name	Settings	SPL	M-ID	SF
Waxman ( $e, d_{max}, \alpha, \beta, m$ )	Wax01	1000,11,0.15,0.2,1	10.71	—	3
	Wax02	2000,20,0.15,0.2,2	4.90	3,4	4
	Wax03	3000,23,0.15,0.2,3	3.97	3,4,5	4
	Wax04	4000,38,0.15,0.2,4	3.52	3,4,5	1
	Wax05	5000,42,0.15,0.2,5	3.26	3,4,5	1
	Wax06	1000,8,0.15,0.2,1	14.54	—	3
	Wax07	2000,15,0.15,0.2,2	5.14	3,4	4
	Wax08	3000,33,0.15,0.2,3	4.01	3,4,5	4
	Wax09	4000,29,0.15,0.2,4	3.56	3,4,5	4
	Wax10	5000,35,0.15,0.2,5	3.29	3,4,5,6	1
Glp ( $e, d_{max}, p, \beta, m$ )	Glp01	1845,108,0.45,0.64,1	3.35	3,6	5
	Glp02	3722,135,0.45,0.64,2	2.98	3,5,6	5
	Glp03	5310,174,0.45,0.64,3	2.79	3,5,6	5
	Glp04	7424,166,0.45,0.64,4	2.66	3,5,6	5
	Glp05	9170,200,0.45,0.64,5	2.56	3,5,6	5
	Glp06	1803,120,0.45,0.64,1	3.32	6	5
	Glp07	3684,152,0.45,0.64,2	2.98	3,5,6	5
	Glp08	5235,174,0.45,0.64,3	2.78	3,5,6	5
	Glp09	7136,178,0.45,0.64,4	2.66	3,5,6	5
	Glp10	9055,210,0.45,0.64,5	2.56	3,5,6	5
Unit-disk graphs ( $e, d_{max}, r, \rho$ )	Adh01	3709,16,50,9.9	15.11	3,5,6	2
	Adh02	4297,17,55,7.9	14.03	3,5,6	2
	Adh03	5183,21,60,2,7.0	12.22	3,5,6	2
	Adh04	6252,26,65,15.4	10.85	3,5,6	2
	Adh05	7227,26,70,20.1	9.86	3,5,6	2
	Adh06	11922,45,70,9.9	6.85	3,5,6	2
	Adh07	13152,48,75,7.9	6.46	3,5,6	2
	Adh08	15790,56,80,7.0	5.84	3,5,6	2
	Adh09	12686,55,70,15.4	6.64	3,5,6	2
	Adh10	14943,65,75,20.1	6.03	3,5,6	2

The Barabási model, as proposed by Barabási *et al.* [4], is used to create the networks Bar01-10 with the Brite topology generator [32]. The Barabási model

captures the preferential attachment, incremental growth, and power law that is observed in the Internet. The probability of any given node  $i$  being connected to another node  $j$  of degree  $d_j$  when joining the network is given by  $P(i, j) = \frac{d_j}{\sum_{k \in V} d_k}$  [32] where  $V$  is the set of nodes already in the network. In Table 6.1, the networks Bar01-Bar10 are described by the settings  $(e, d_{max}, m)$  where  $e$  represents the number of edges,  $d_{max}$  the maximum out degree, and  $m$  the number of edges assigned for each new node.

An extended Barabási model is used to create the networks Bar11-Bar20 [56, 1]. Each network is described by the settings  $(e, d_{max}, p, q, m)$  in Table 6.1 with  $p$  and  $q$  representing the connection probabilities used with the Brite topology generator [32].

The Waxman model proposed in [47] is used to create networks Wax01-Wax10. This model is a variant of the Erdős-Renyi random graph model in [11] with extra characteristics that are network specific. The probability of connecting two nodes is  $P(i, j) = \alpha e^{\frac{-l}{\beta l_{max}}}$  where  $l$  is the distance between the two nodes;  $i$  and  $j$ ,  $l_{max}$  is the maximum distance between any two nodes in the network and  $0 < \alpha, \beta \leq 1$  [32]. The created networks (Wax01-Wax10) are described by the settings  $(e, d_{max}, \alpha, \beta, m)$  in Table 6.1.

The networks Tdn01-Tdn10 are created using a top-down hierarchical model that simulates the Internet structurally with two levels consisting of an *autonomous system* (AS) level and a router network level [13, 32]. The networks are described by the settings  $(e, d_{max}, u, d)$  in Table 6.1 where  $u$  refers to the number of AS's and  $d$  refers to the number of routers assigned to each AS. The routers within each AS are created using the Waxman model defined earlier with  $\alpha = 0.15, \beta = 0.2$ .

The Generalized Linear Preferential (GLP) model is used to create the networks Glp01-Glp10 [12]. The settings  $(e, d_{max}, p, \beta, m)$  in Table 6.1 are used to describe the settings for networks Glp01-Glp10 using Brite topology generator [32].

A unit disk graph model is used to create the networks Adh01-Adh10 [16]. In this model, a node is connected to every node within a distance of  $r$  units by an edge while ensuring that the ensuing graph is fully connected. The settings  $(e, d_{max}, r, \rho)$  in Table 6.1 describe the networks where  $\rho$  is taken to be the clustering coefficient of the network.

To complement our results, we also investigate three networks derived from the Caida project [42]. Because these networks are observed in the actual Internet and not created using any mathematical model, we have no control over their size. These networks are bigger, of different sizes, and not completely connected, which means that their scheme performance cannot be directly compared with each other or the other 60 networks. Therefore, we simply discuss their results in Section 7.6. Caida1-3 are the complementary networks derived from the Caida project [42]. Caida1 has 3451 nodes and 4048 edges, Caida2 has 3537 nodes and 4150 edges, while Caida3 has 3527 nodes and 4143 edges. The attack simulations carried out in these networks also consisted of 50 randomly selected attackers sending traffic to one victim and their results are averaged over 100 simulations.

## CHAPTER 7

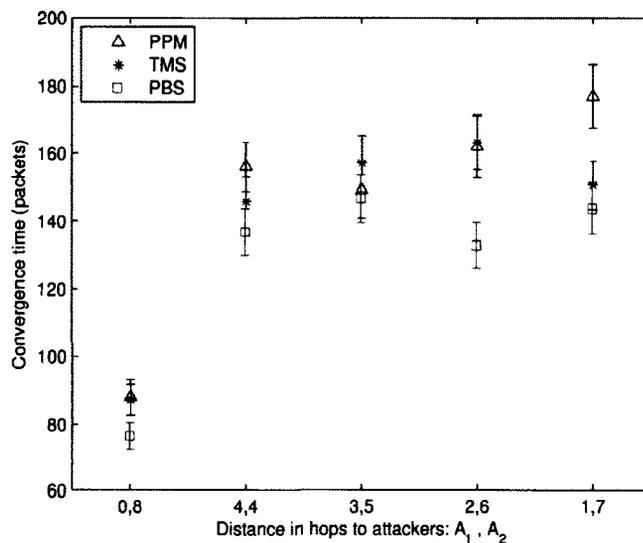
### RESULTS AND DISCUSSION

#### 7.1 Average Path Length

In this subsection, we show using a simplified attack graph that scheme performance varies significantly even when the average attack path's length is constant. We consider a V-shaped attack graph consisting of two attackers,  $A_1$  and  $A_2$ , that send their traffic to the victim  $V$  (cf. Figure 4.2). We measure the convergence time for the considered schemes with varying attack path lengths while keeping the average path's length constant.

Figure 7.1 shows the convergence times for PPM, TMS and PBS in five V-shaped attack graphs, which all exhibit an average attack path length of four hops. Each attack graph is represented by  $(l_1, l_2)$  where  $l_1$  and  $l_2$  are the distances in hops between  $V$  and the attackers  $A_1$  and  $A_2$ , respectively. The figure shows that despite identical average path's lengths between the attack graphs, each attack graph exhibits differing scheme performance and ranking of performance. For example, an attack graph of equal path lengths, represented by  $(4, 4)$ , exhibits a range of 20 packets among the convergence times with  $\text{PPM} > \text{TMS} > \text{PBS}$ . In contrast, an attack graph of different path lengths, represented by  $(2, 6)$ , exhibits a range of 30 packets with  $\text{TMS} > \text{PPM} > \text{PBS}$ . The attack graph represented by  $(1, 7)$  in Figure 7.1 exhibits a

range of 35 packets with  $PPM > TMS > PBS$ . These results are more dramatic when one considers that this specific scenario only consists of two attackers who are close to the victim (less than eight hops) when typical DDoS attacks have thousands of attackers located up to 25 hops away from the victim.



**Figure 7.1:** Convergence times for five V-shaped 2-attacker graphs of equal average length, with 95% confidence intervals. This plot shows that even with identical values for average path length, the distance of the attackers relative to each other affects the considered schemes in different ways

In the context of a larger network, these results show that variation in scheme performance can be expected in larger networks even if those networks exhibit similar average shortest path values.

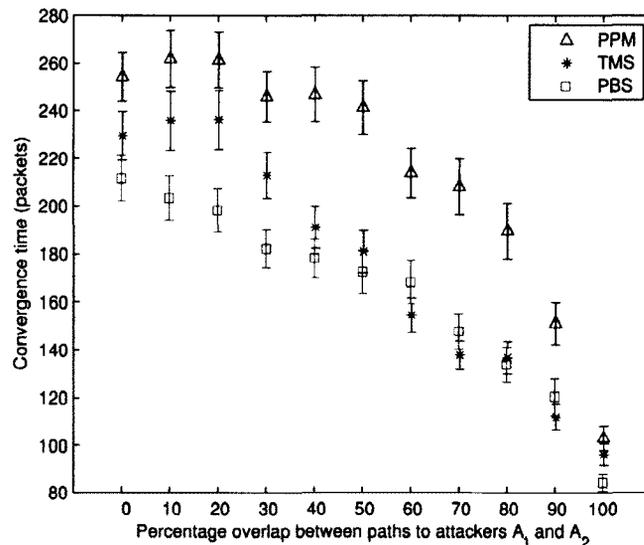
## 7.2 Overlapping of Attack Paths

In this subsection, we show how the level of overlap between two attack paths affects the schemes' convergence times. We consider a Y-shaped attack graph linking attackers  $A_1$  and  $A_2$  to victim  $V$  (cf. Figure 4.3). While keeping each attack path

equal and constant, we vary the amount of overlap between the attack paths and observe how the convergence times of PPM, TMS, and PBS are affected.

Figure 7.2 shows the observed results from this investigation. The results show that there is a general reduction in convergence times for all considered schemes as the percentage overlap is increased. Despite the general reduction for all three considered schemes, the level of overlap affects each scheme uniquely. For example, the results show that PPM and TMS are relatively unaffected by low amounts of overlap, i.e. 0-20%, while PBS exhibits a reduction in convergence times in the same overlap range. However, further increase in percentage overlap causes a drastic decrease in the convergence time of TMS such that by 60%-70% TMS has lower convergence times than both PBS and PPM. These results show three things: Firstly, larger amounts of overlapping attack paths translates to reduced convergence times; Secondly, low amounts of overlapping attack paths affects PBS more than PPM and TMS; and thirdly, medium amounts of overlapping cause a drastic reduction in TMS convergence times.

In the context of a larger network, these results mean that even for long path lengths, the existence of common and therefore overlapping attack paths translates to reduced convergence times for TMS and PBS more than it does for PPM. This is because the overlaps, which are typically downstream, result in increased probabilities for the least likely edges for PBS and TMS, which in turn leads to lower convergence times.



**Figure 7.2:** Convergence times for 11 Y-shaped 2-attacker graphs of equal average length, with 95% confidence intervals. This plot shows that the convergence time of the considered schemes is affected by the percentage of the attack path that is common to more than one attacker

### 7.3 Occurrence of Motifs in Attack Graphs

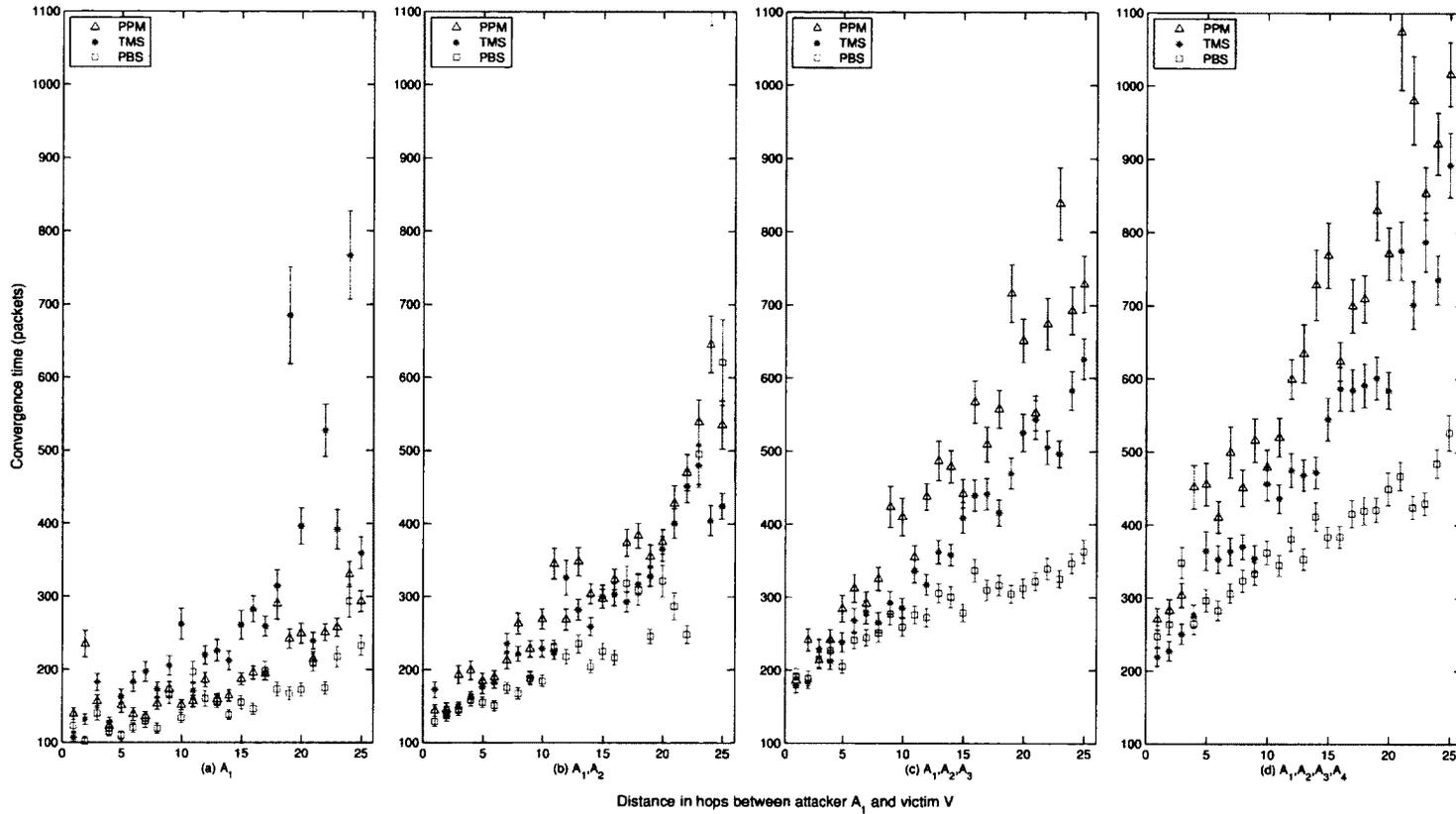
In this subsection, we show how the existence of a subgraph in an attack graph has a unique influence on different schemes' performances. We consider a Q-shaped attack graph that links an attacker  $A_1$  to victim  $V$  and contains Subgraph 4 (cf. Figure 4.5). We use the Q-shaped attack graph to understand how the presence of alternative paths affects the convergence times of different schemes. In this scenario, the alternative path is the same length as the original path. The tendency of network traffic to take alternative routes also depends on the amount of traffic being processed and therefore we consider up to three other attackers contributing an equivalent amount of traffic. Including other attackers in the Q-shaped attack graph allows us to see whether the amount of traffic affects the convergence times of the considered schemes.

Figure 7.3 shows the convergence times for four different kinds of Q-shaped attack graphs. In each case, the path length to attacker  $A_1$  is varied between 3 and 27 hops (distance of 1-25 hops from the subgraph) and the convergence times for PPM, TMS and PBS are measured. In Figure 7.3(a), we only consider  $A_1$ . In Figure 7.3(b), we introduce  $A_2$  at a distance of 3 hops from the victim as in Figure 4.5 and observe if this changes the observations of Figure 7.3(a). In Figure 7.3(c) and (d), we introduce attackers  $A_3$ , and  $A_4$  respectively to show how increased traffic from other attackers affects our results. The path distance to attackers  $A_2$ ,  $A_3$  and  $A_4$  is constant at 3 hops from the victim, while  $A_1$ 's path distance is varied in each case.

Figure 7.3(a) shows the convergence times with just attacker  $A_1$ . As expected, all schemes exhibit a general increase in convergence times with longer attack path length. However, PPM's convergence times are the least affected by the increase in path length, particularly for path lengths longer than 15 hops. In contrast, TMS exhibits comparatively high convergence times for path lengths longer than 15 hops.

When another attacker  $A_2$  is included as in Figure 7.3(b), there is a general increase in convergence times, which is due to the increase in the size of attack graph. However, the TMS convergence times for path lengths longer than 15 hops is now comparable to the PPM and PBS convergence times. Additionally, PPM convergence times for path lengths longer than 15 hops is now more responsive to a path's length than it was in Figure 7.3(a) when there was only one attacker.

Including attacker  $A_3$  yields the results in Figure 7.3(c). While there is a general increase in convergence times from Figure 7.3(b) to Figure 7.3(c), PBS convergence times are considerably less than PPM and TMS for path lengths longer than 15 hops.



**Figure 7.3:** Convergence times for a Q-shaped attack graph under varying conditions, with 95% confidence intervals. Within each plot, the distance of attacker  $A_1$  from the subgraph at victim  $V$  is varied from 1 hop to 25 hops. Between each plot, the number of attackers is increased by one, i.e. Figure (a) just considers traffic from  $A_1$ , Figure (b) considers traffic from  $A_1$  and  $A_2$ , Figure (c) considers  $A_1$ ,  $A_2$ , and  $A_3$ , while Figure (d) considers  $A_1, A_2, A_3$  and  $A_4$ . These plots show that the motif in the attack graph has a distinct influence on the convergence time of different marking schemes and this influence also varies with the number of attackers in the graph

Additionally, PPM now exhibits the highest convergence times of the three considered schemes.

Including attacker  $A_4$  yields the results in Figure 7.3(d). As in Figure 7.3(c), PBS generally exhibits the lowest convergence times while PPM exhibits the highest. Additionally, the PBS convergence times do not seem as responsive to an increase in path length for paths longer than 15 hops.

These results show that the subgraphs in an attack path have a higher impact on the performance of TMS and PBS than on PPM, particularly when other attackers do not contribute traffic to the subgraph. However, when other attackers are considered, the increased traffic in the subgraph offsets this impact leading to lower convergence times for TMS and PBS than for PPM.

In the context of a larger network, these results show that the effect of subgraphs in attack graphs depends on how many attack paths have merged by the time the subgraph is encountered. As the number of attackers increases, as in a DDoS attack, we expect significantly higher PPM convergence times than TMS and PBS. With a low number of attackers, the subgraphs in the attack paths lead to high TMS convergence times compared to PPM and PBS. Additionally, networks with long average paths should exhibit large discrepancies between PPM performance on one hand, and PBS and TMS performance on the other hand.

## 7.4 Motifs and SRPs

In this subsection, we present the results obtained in the process of network classification. We present the identified network motifs and the derived superfamilies, as well as all intermediate results obtained in the process.

The 4-node motifs identified in all the considered networks are presented in the M-ID column of Table 6.1. The table shows that 14 out of the 60 networks do not exhibit any network motifs. This means that while the networks exhibit all six 4-node undirected subgraphs, the frequency of these subgraphs is not significantly high enough to warrant any of the subgraphs being identified as a motif of that network. The table also shows that many networks exhibit multiple network motifs. The network motifs exhibited by a network provide an indication of what kind of subgraphs are likely to appear in a DDoS attack graph derived from that network. For example, Bar11 exhibits subgraphs 3, 4, and 5 as network motifs. Therefore, DDoS attack graphs in the Bar11 network are more likely to exhibit subgraphs 3, 4, or 5 compared to any other 4-node subgraphs.

Figure 7.4(a) shows the significance ratio profiles (SRPs) for all 60 considered networks. The SRPs can be used to show the relative abundance or absence of all six 4-node subgraphs and consequently derive the superfamilies within the networks based on their structural similarity. The figure shows that the majority of the networks exhibit average amounts of subgraphs 1 and 2. In contrast, the networks exhibit different levels of prevalence for subgraphs 3, 4, 5, and 6, which coincidentally are the subgraphs that contain alternative routes.

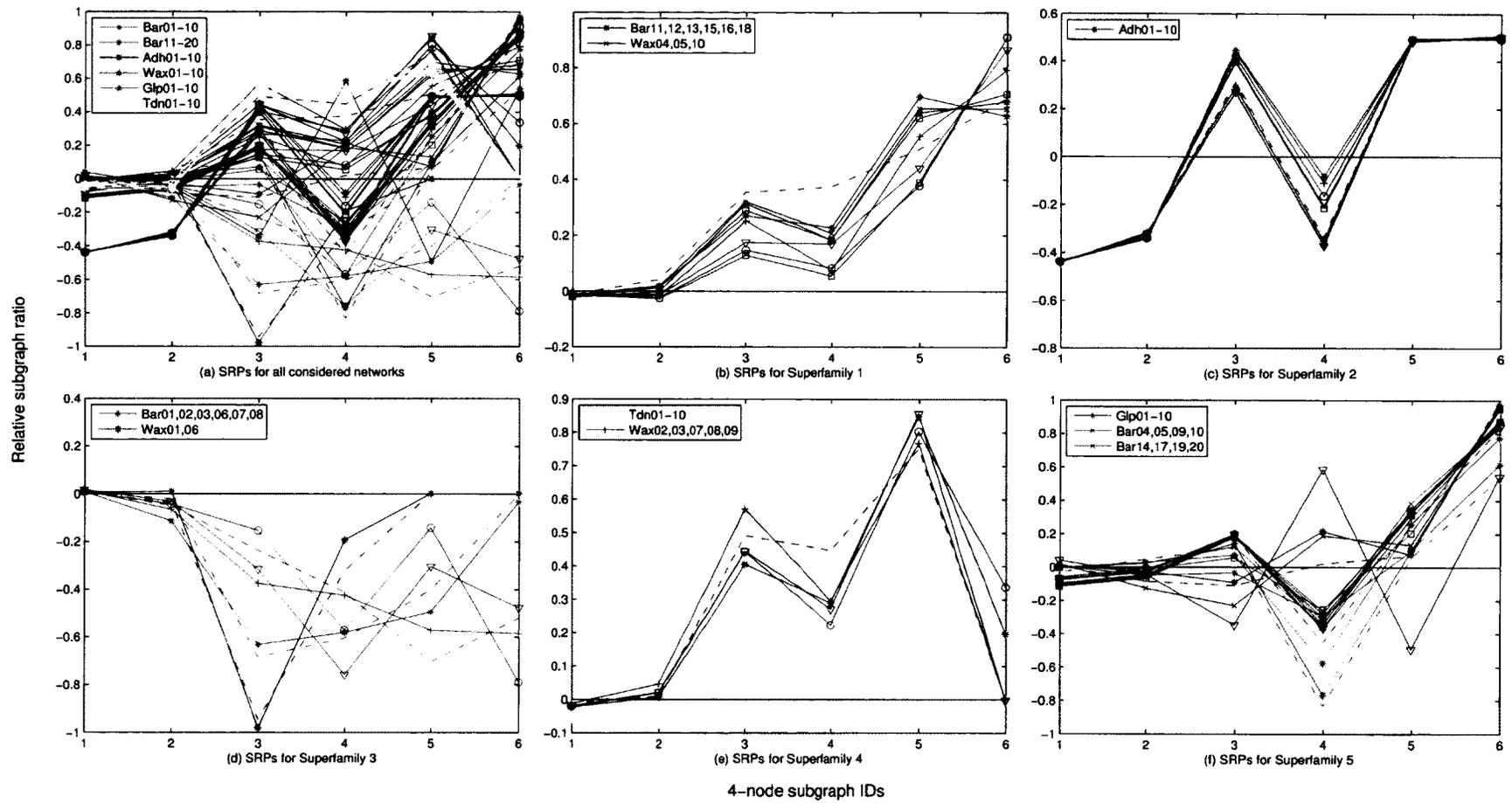
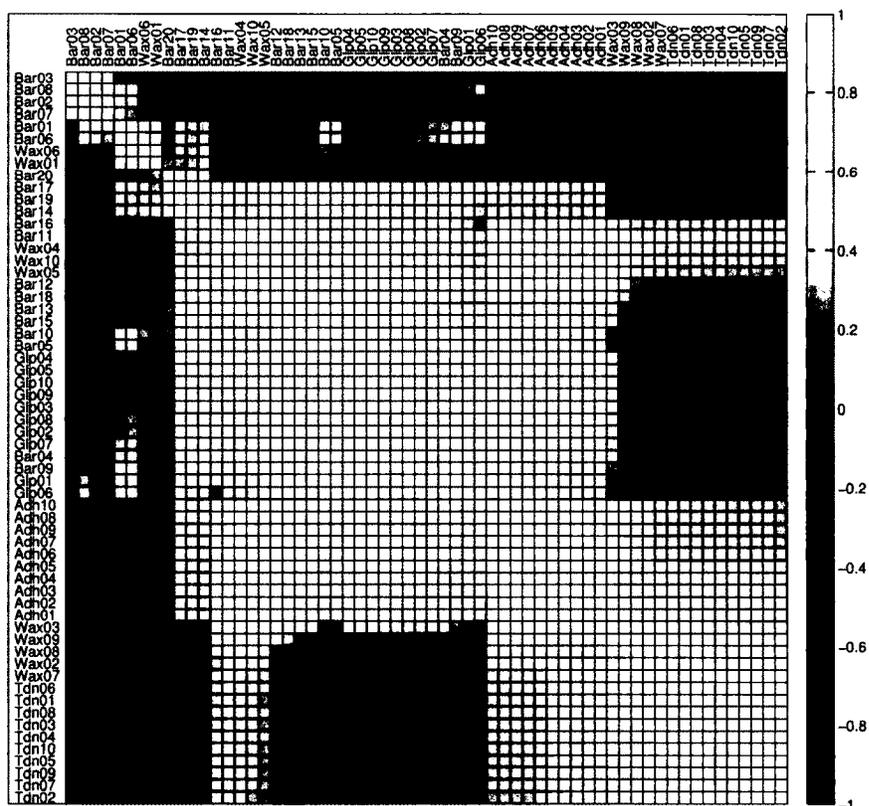


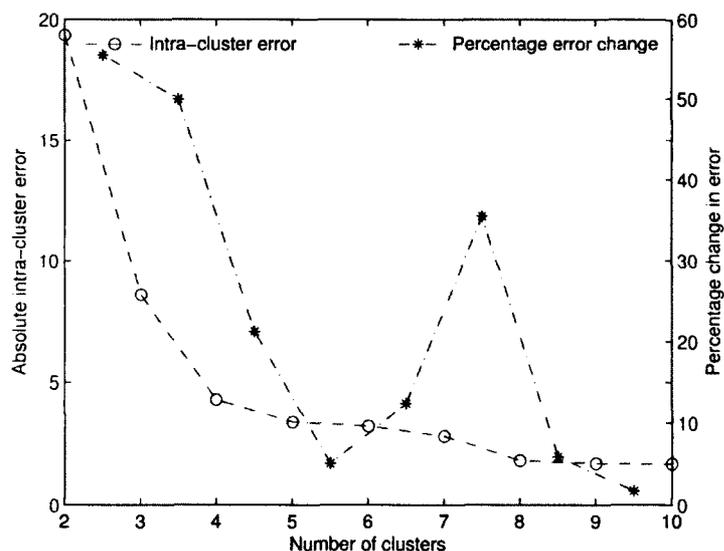
Figure 7.4: Subgraph ratio profiles (SRPs) for all networks as well as the five identified superfamilies

We use Figure 7.5 to obtain an impression of the superfamilies contained within the considered networks. The figure shows a color-coded correlation map of the SRPs with light colored squares representing high correlation values, while dark colored squares represent low correlation values. A cluster of light colored squares provides a visual indication of a possible superfamily since the SRPs are very similar, and consequently the represented networks are structurally similar. This figure shows 3-4 possible superfamilies. For example, the TDN networks are very similar to the ADH networks as well as five Wax networks and could all possibly belong to one superfamily.



**Figure 7.5:** Correlation map for the network SRPs arranged by similarity. The correlation map shows the levels of similarity between the different network SRPs and is used to give a visual indication of how many groups the networks can be placed into

We use Figure 7.6 to obtain a more accurate number of clusters. By plotting the intra-cluster error against the possible number of clusters, we are able to identify an appropriate number of clusters. The number of clusters should exhibit a low intra-cluster error. Additionally, the percentage change in error when one increases the number of clusters by one should be minimal. From Figure 7.6, we deduce that the 60 networks can be placed into five clusters, hereafter referred to as superfamilies. This is because five clusters exhibits a lower error than four clusters, and also exhibits a percentage difference in error that is less than a predetermined tolerance level of 10%. This value allows us to find a balance between cluster size and error.



**Figure 7.6:** The cluster decision plot which shows intra-cluster error  $e(m)$  and percentage change in error  $\frac{e(m+1)-e(m)}{e(m)}$  versus number of clusters  $m$ . The percentage change in error is used to quantify the benefit of increasing the number of clusters from  $m$  to  $m + 1$ . The cluster decision plot is used to determine an accurate ideal number of clusters from the SRPs of the networks

The SRPs of the five identified superfamilies are shown in Figure 7.4(b)-(f).

The SRPs within each superfamily are similar to each other, and yet different from

the SRPs in other superfamilies. Therefore, the networks within each superfamily are structurally similar to each other, and yet distinct from other superfamilies.

### 7.5 Overall IP Traceback Performance

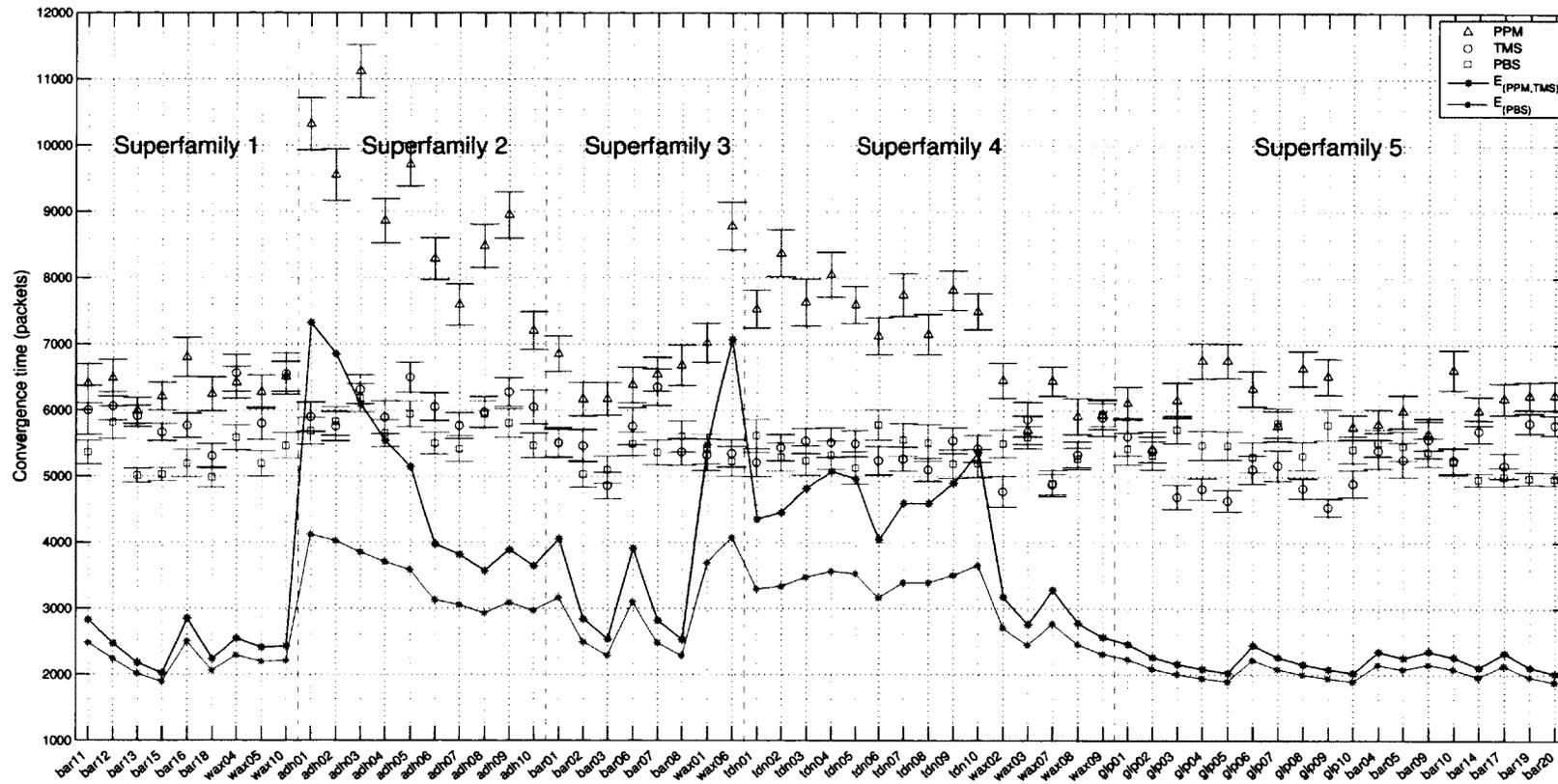
In the preceding subsections, we demonstrate the individual influence of three topology-based factors that affect the performance of PPM-based schemes in large scale networks. In each of the subsections, the attack graphs are designed to illustrate and emphasize those specific factors. In this subsection, we evaluate the performance of selected schemes in a large set of Internet-like networks to observe the schemes' performances in more realistic scenarios. In contrast to the attack graphs in the previous sections, we have limited control over the shape and structure of these attack graphs. This allows us to observe the collective influence of all topology-dependent factors in an unbiased manner. Therefore, by evaluating the schemes in these networks, we are able to show how all the previous mentioned factors combine to affect the performance of PPM, TMS, and PBS in more realistic scenarios than considered in preceding subsections.

Figure 7.7 shows the average PPM, TMS and PBS convergence times in 60 different networks, which are all the same size. Each network is subjected to 200 different DDoS attacks of the same scale under each of the three considered schemes. The convergence times are measured and averaged to provide an indication of the schemes' performance in each network. Given the similarity in network size and attack scale, the observed differences in convergence time can be solely attributed to subtle

differences in graph structure among the different networks, and the way the graph structure affects each marking scheme uniquely.

The first observation from this graph is that the convergence times for all three considered schemes vary from one network to another. In fact, even the ranking of performance of the schemes also varies with the network. For example, Bar11 exhibits PPM>TMS>PBS while Wax04 exhibits TMS>PPM>PBS and Tdn06 exhibits PPM>PBS>TMS. Despite the variation in scheme performance, the plot shows that PPM generally exhibits a higher convergence time than both TMS and PBS.

Another observation from this graph is the difference between PPM convergence times on one hand, and TMS and PBS convergence times on the other hand. In some networks, all three schemes exhibit similar convergence times. For example, network Wax09 exhibits a difference between the best and worst performing schemes of 298.36 packets. In contrast, network Adh03 exhibits a difference between the best and worst performing schemes of 6094.79 packets. This discrepancy shows that the underlying topologies affect different schemes in different ways. In some topologies, all the schemes are comparable in performance, while scheme performances are vastly different in other topologies. The fact that TMS and PBS convergence times seem fairly stable among different networks while PPM convergence times are erratic shows that PPM is more vulnerable to the structural differences between different networks.



**Figure 7.7:** Convergence times for PPM, TMS, and PBS, with their 95% confidence intervals, in 60 different networks arranged according to the superfamily they belong to. The line plots (shown in black and purple) show the expected convergence times for the schemes as evaluated using the traditional analytical models and the networks' average shortest path values (cf. Table 2.2 and Section 5.1). The black line plot shows the expected convergence times for PPM and TMS, while the purple line plot shows PBS' expected convergence time. The plot shows that the convergence time for the different schemes varies from one network to another, and in most networks exceeds the expected convergence time based on analytical models. Furthermore, this plot shows that the best performing scheme in one network is not necessarily the best performing scheme in another network

It is interesting to note that when the networks are arranged by a superfamily, the networks within each superfamily tend to exhibit similar scheme performances. For example, Superfamilies 1 and 5 exhibit low ranges between their best and worst performing schemes regardless of the fact that they consist of networks created using different mathematical models. In contrast, superfamilies 2, 3, and 4 exhibit large ranges between their best and worst performing schemes. This observation indicates that there is a link between the structural similarity as captured using the superfamily technique, and the performance of PPM-based schemes in different networks.

The adjusted model (cf. Section 5.2) shows that alternative routes in attack paths, such as those offered by Subgraphs 3, 4, 5, and 6, have the effect of increasing convergence times for all considered schemes. However, the merging of different attack streams cancels out this effect particularly in TMS and PBS where this merging also reduces the convergence times (cf. Section 5.3). This leads to a discrepancy in results between PPM on one hand, and TMS and PBS on the other hand. This discrepancy in results between the schemes is more pronounced with more alternative paths, and therefore Subgraph 6 has a larger effect than Subgraph 3 since Subgraph 6 has four alternative routes compared to Subgraph 3 which only has two alternative routes. We therefore expect to see increased discrepancy between PPM convergence times and both TMS and PBS convergence times for networks with an abundance of Subgraphs 3, 4, 5, and 6, e.g. Glp07-10, Adh01-10. We also expect this discrepancy to be more pronounced with Subgraphs 5 and 6 than it is with Subgraphs 3 and 4.

Our results agree with the presented model. In Figure 7.7, convergence times for TMS and PBS in Superfamilies 2 and 4 are generally similar to Superfamilies 1, 3

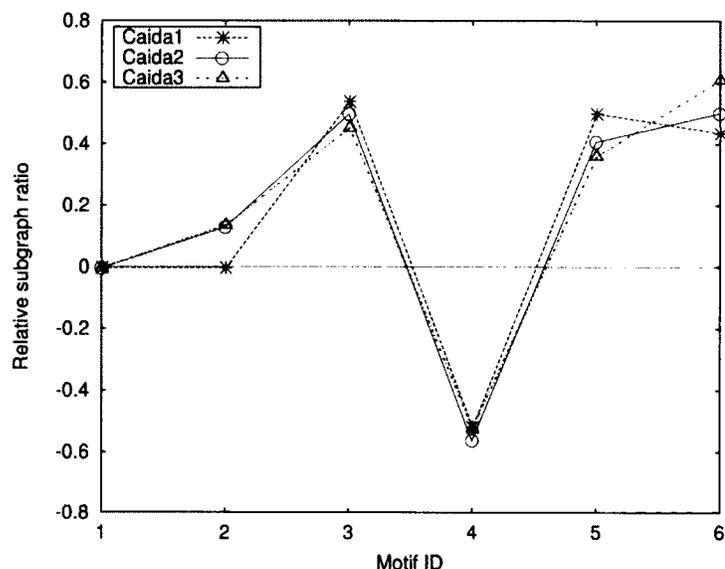
and 5 despite the increase in average shortest path length, while the convergence times for PPM are higher. Additionally, Superfamily 2 shows the most difference between PPM, and TMS and PBS, because it has an abundance of Subgraph 6, as shown in Figure 7.4c, and identified in Table 6.1. This result validates the model presented earlier and shows how the motifs affect scheme convergence time uniquely.

Note that networks built from the same model can belong to different superfamilies, and exhibit different scheme performances. This indicates that the superfamily technique can be used as a means to identify possible networks with similar network protocol performance even when the networks have differing construction principles or models. This observation calls for more research with other network protocols to determine whether networks belonging to the same superfamily exhibit similar performance regardless of the mathematical models used to create them.

## 7.6 Caida Networks

In this section, we present complementary results derived from the three networks from the Caida project [42] referred to as Caida1, Caida2, and Caida3.

The SRPs for all three networks are shown in Figure 7.8. The figure reveals that all three Caida networks have very similar SRPs and yet these SRPs are distinct from the SRPs in Figure 7.4. The networks exhibit a lack of Subgraph 4, an abundance of subgraphs 3, 5 and 6, as well as average amounts of Subgraphs 1 and 2.



**Figure 7.8:** The subgraph ratio profiles (SRPs) of the three Caida networks. These networks are similar to each other and yet different from the SRPs of the five superfamilies

The convergence times for the attacks carried out in these networks are presented in Table 7.1 alongside their 95% confidence intervals. The table shows that  $PPM > TMS > PBS$  for all three networks. As expected, TMS and PBS convergence times are similar to each other, and yet distinct from PPM convergence times for all three networks. It is interesting to point out that even though these networks are at least three times the size of the other 60, the TMS and PBS convergence times are comparable to the rest. Additionally, PPM convergence times are comparable to the convergence times of the networks in Superfamily 2. One would expect that the convergence times for all schemes would drastically increase with an increase in the network size. The link between network size and protocol performance presents an interesting direction for future research.

**Table 7.1:** The average convergence times, measured in packets, for the three Caida networks as well as their 95% confidence intervals after 100 simulations

<b>Network</b>	<b>PPM</b>	<b>TMS</b>	<b>PBS</b>
Caida1	6503.9 $\pm$ 357.54	5090.3 $\pm$ 266.61	4858.5 $\pm$ 281.61
Caida2	7126.4 $\pm$ 392.97	5932.8 $\pm$ 494.89	5689.0 $\pm$ 232.08
Caida3	6631.6 $\pm$ 391.62	5551.5 $\pm$ 347.11	5506.6 $\pm$ 231.84

## CHAPTER 8

### CONCLUSIONS AND FUTURE WORK

#### 8.1 Conclusions

In the first part of this dissertation, we present two enhancements to improve the PPM traceback schemes. First, we present a novel marking scheme that allows complete traceback with decreased convergence time. Second, we extend an existing traceback algorithm by a prediction component.

The proposed marking scheme ensures that packet markings from different sections of the attack path have the same chance of arriving at the victim. Additionally, the proposed traceback algorithm has a prediction component, which builds graphs based on legitimate traffic collected prior to or after an attack. A feature of this extended traceback algorithm is to predict the attack packets' paths without receiving markings from all routers in the path.

Results show that the marking scheme makes it possible for complete graph construction with 54% of the total packets required with traditional techniques. The prediction component in the traceback algorithm also allows for complete traceback to be possible with 33% of the usual number of marked packets.

Both techniques can be used independently to improve existing techniques based on PPM.

In the second part of this dissertation, we study the influence of network topology on the performance of PPM-based schemes. We identify three network-dependent factors and show empirically that they uniquely affect different PPM-based schemes leading to possible discrepancy in the schemes' performances from one network to another. Additionally, by implementing selected schemes on an extensive set of Internet-like topologies, we are able to show the collective contribution of these factors to scheme performance in more realistic deployment scenarios than previously considered. Network motifs and subgraph ratio profiles are applied to capture the subtle differences and similarities in structure between these topologies and to assign them to superfamilies.

Our results show a strong dependence of PPM-based scheme performance on network structure. Our results also show that networks that are similar according to the network motif technique exhibit similar PPM-based scheme performance. Moreover, an analytical model is presented in this dissertation, which shows how this link affects the schemes uniquely, contributing to the discrepancies in their convergence times among the networks.

The presented results raise questions about other network protocols that have typically assumed an independence from the network structure on which they are implemented. Our work encourages multiple network evaluation of such protocols to provide performance guarantees in large scale networks similar to the Internet. To that end, our work also presents a network clustering process that can be used to group Internet-like networks into superfamilies according to their structural similarity.

A network protocol could potentially be tested in one representative network from each superfamily instead of testing it on all possible networks.

## 8.2 Future Work

Possible future work includes designing motif-aware protocols and schemes. Given that this work shows that PPM-based schemes are dependent on the networks in which they are implemented, and more specifically, dependent on the motifs exhibited by those networks, it stands to reason that these dependencies could be exploited for improved performance. Such schemes would ideally exhibit the best performance in all networks belonging to a specific superfamily, or networks exhibiting a specific network motif.

Another direction for future research involves multiple network evaluation and comparison of network protocols as opposed to the common practice of analyzing a protocol in a single type of network. Previous research assumed that PPM-based schemes were independent of the underlying networks, which meant that single network evaluation was adequate to capture and compare scheme performance. It follows that other network protocols should also be evaluated on a large set of representative networks in order to make accurate performance guarantees.

## BIBLIOGRAPHY

- [1] R. Albert and A. L. Barabási. Topology of evolving networks: local events and universality. *Physical review letters*, 85(24):5234–5237, 2000.
- [2] B. Augustin, T. Friedman, and R. Teixeira. Measuring load-balanced paths in the internet. In *Proc. of ACM SIGCOMM Conf. on Internet Measurement*, pages 149–160, San Diego, CA, USA, 2007.
- [3] R. Banner and A. Orda. Multipath routing algorithms for congestion minimization. *IEEE/ACM Trans. on Networking*, 15(2):413–424, 2007.
- [4] A. L. Barabási and R. Albert. Emergence of scaling in random networks. *Science*, 286(5439):509–512, 1999.
- [5] BBC-Online. 123-reg hosted websites go offline after 'china attack', 2012. <http://www.bbc.com/news/technology-18179298>. Date of publication: May 23, 2012. Date retrieved: May 24, 2012.
- [6] BBC-Online. Anonymous attacks indian government websites, 2012. <http://www.bbc.com/news/technology-18114984>. Date of publication: May 18, 2012. Date retrieved: May 24, 2012.
- [7] BBC-Online. Soca website attack: Norway arrests two youths, 2012. <http://www.bbc.com/news/technology-18005505>. Date of publication: May 9, 2012. Date retrieved: May 24, 2012.
- [8] A. Belenky and N. Ansari. Ip traceback with deterministic packet marking. *Comm. Letters, IEEE*, 7(4):162–164, 2003.
- [9] A. Belenky and N. Ansari. On ip traceback. *IEEE Comm. Magazine*, 41(7):142–153, 2003.
- [10] S. Bellovin, M. Leech, and T. Taylor. *ICMP traceback messages*. Internet Engineering Task Force, 2003.

- [11] B. Bollobas. *Random Graphs*. Cambridge University Press, 2001.
- [12] T. Bu and D. Towsley. On distinguishing between internet power law topology generators. In *Proc. of IEEE INFOCOM Conf.*, New York, USA.
- [13] K. L. Calvert, M. B. Doar, and E. W. Zegura. Modeling internet topology. *IEEE Communications Magazine*, 35(6):160–163, 1997.
- [14] Carnegie Mellon University (CERT). Denial of service attacks, 2014. [http://www.cert.org/historical/tech\\_tips/denial\\_of\\_service.cfm](http://www.cert.org/historical/tech_tips/denial_of_service.cfm). Date accessed: May 28, 2014.
- [15] C.-Y. Cheng, C.-Y. Huang, and C.-T. Sun. Mining bridge and brick motifs from complex biological networks for functionally and statistically significant discovery. *IEEE Trans. on Systems, Man, and Cybernetics, Part B: Cybernetics*, 38(1):17–24, 2008.
- [16] B. N. Clark, C. J. Colbourn, and D. S. Johnson. Unit disk graphs. *Discrete Mathematics*, 86(13):165–177, 1990.
- [17] I. Cunha, R. Teixeira, and C. Diot. Measuring and characterizing end-to-end route dynamics in the presence of load balancing. In *Proc. of the Int. Conf. on Passive and Active Measurement*, pages 235–244, Atlanta, GA, USA, 2011.
- [18] Digital Attack Map. Top daily ddos attacks worldwide, 2014. <http://www.digitalattackmap.com/gallery/>. Date accessed: May 29, 2014.
- [19] M. El Dayeh and M. Hahsler. Biological pathway completion using network motifs and random walks on graphs. In *IEEE Symp. on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB)*, pages 229–236, San Diego, CA, USA, 2012.
- [20] M. Faloutsos, P. Faloutsos, and C. Faloutsos. On power-law relationships of the internet topology. In *ACM SIGCOMM*, pages 251–262, Cambridge, MA, USA, 1999.
- [21] W. Feller. *An Introduction to Probability Theory and Its Applications*. Wiley, 1968.

- [22] Z. Gao and N. Ansari. Tracing cyber attacks from the practical perspective. *IEEE Comm. Magazine*, 43(5):123–131, 2005.
- [23] M. T. Goodrich. Probabilistic packet marking for large-scale ip traceback. *IEEE/ACM Trans. Netw.*, 16(1):15–24, 2008.
- [24] D. Hales and S. Arteconi. Motifs in evolving cooperative networks look like protein structure networks. In *Proc. of the European Conf. on Complex Systems*, Dresden, Germany, 2007.
- [25] I. Kaj and R. Gaigalas. Waxman random network topology generator, 2005. <http://www2.math.uu.se/research/telecom/software/>. Date of last revision: December 2005. Date retrieved: May 24, 2012.
- [26] A. R. Kiremire, M. R. Brust, and V. V. Phoha. A prediction based approach to ip traceback. In *Proc. of the IEEE Conf. on Local Computer Networks*, pages 1022–1029, Clearwater, FL, USA, 2012.
- [27] A. R. Kiremire, M. R. Brust, and V. V. Phoha. Topology-dependent performance of attack graph reconstruction in ppm-based ip traceback. In *Proc. of the IEEE Conf. on Consumer Communications and Networking*, Las Vegas, NV, USA, 2014.
- [28] A. R. Kiremire, M. R. Brust, and V. V. Phoha. Using network motifs to investigate the influence of network topology on ppm-based ip traceback schemes. *Elsevier Journal on Computer Networks*, 2014.
- [29] J. Li, M. Sung, J. Xu, and L. Li. Large-scale ip traceback in high-speed internet: practical techniques and theoretical foundation. In *Proc. of IEEE Symp. on Security and Privacy*, pages 115–129, Berkeley, CA, USA, 2004.
- [30] M. Ma. Tabu marking scheme to speedup ip traceback. *Computer Networks*, 50(18):3536–3549, 2006.
- [31] D. Marcus and Y. Shavitt. Efficient counting of network motifs. In *Proc. of IEEE Int. Conf. on Distributed Computing Systems Workshops (ICDCSW)*, pages 92–98, Genoa, Italy, 2010.

- [32] A. Medina, A. Lakhina, I. Matta, and J. Byers. Brite: An approach to universal topology generation. In *Proc. of the Int. Symp. in Modeling, Analysis and Simulation of Computer and Telecom. Systems*, Cincinnati, OH, USA, 2001.
- [33] R. Milo, S. Itzkovitz, N. Kashtan, R. Levitt, S. Shen-Orr, I. Ayzenshtat, M. Sheffer, and U. Alon. Superfamilies of evolved and designed networks. *Science*, 303(5663):1538–1542, 2004.
- [34] R. Milo, S. Shen-Orr, S. Itzkovitz, N. Kashtan, D. Chklovskii, and U. Alon. Network motifs: Simple building blocks of complex networks. *Science*, 298(5594):824–827, 2002.
- [35] The Network Simulator NS-2. <http://www.isi.edu/nsnam/ns/>.
- [36] V. Paruchuri, A. Durrezi, and S. Chellappan. Ttl based packet marking for ip traceback. In *Proc. of IEEE GLOBECOM Conf.*, pages 1–5, New Orleans, LA, USA, 2008.
- [37] V. Paxson. End-to-end routing behavior in the internet. *ACM SIGCOMM*, 36(5):41–56, 2006.
- [38] S. Savage, D. Wetherall, A. Karlin, and T. Anderson. Practical network support for ip traceback. *ACM SIGCOMM*, 30(4):295–306, 2000.
- [39] D. X. Song and A. Perrig. Advanced and authenticated marking schemes for ip traceback. In *Proc. of IEEE INFOCOM Conf.*, pages 878–886, Anchorage, AK, USA, 2001.
- [40] R. Stone. Centertrack: an ip overlay network for tracking dos floods. In *Proc. of USENIX Security Symp.*, pages 15–15, Denver, CO, USA, 2000.
- [41] H. Tangmunarunkit, R. Govindan, S. Jamin, S. Shenker, and W. Willinger. Network topologies, power laws, and hierarchy. *ACM SIGCOMM Comput. Commun. Rev.*, 32(1):76, 2002.
- [42] The Cooperative Association for Internet Data Analysis (CAIDA). The IPv6 AS Links Dataset - <Jan 01-05, 2014>. [http://www.caida.org/data/active/ipv6\\_aslinks\\_dataset.xml](http://www.caida.org/data/active/ipv6_aslinks_dataset.xml). Date retrieved: April 02, 2014.

- [43] D. A. Tran and H. Raghavendra. Congestion adaptive routing in mobile ad hoc networks. *IEEE Trans. on Parallel and Distributed Systems*, 17(11):1294–1305, 2006.
- [44] Y. K. Tseng, H. H. Chen, and W. S. Hsieh. Probabilistic packet marking with non-preemptive compensation. *IEEE Comm. Letters*, 8(6):359–361, 2004.
- [45] Venture Beat (VB). Ddos attacks in 2014: Smarter, bigger, faster, stronger, 2014. <http://venturebeat.com/2014/04/20/ddos-attacks-in-2014-smarter-bigger-faster-stronger/>. Date accessed: May 29, 2014.
- [46] D. J. Watts and S. H. Strogatz. Collective dynamics of ‘small-world’ networks. *Nature*, 393(6684):440–442, 1998.
- [47] B. Waxman. Routing of multipoint connections. *IEEE Journal on Selected Areas in Comm.*, 6(9):1617–1622, 1988.
- [48] A. Whalen, S. Brennan, T. Sauer, and S. Schiff. Observability of neuronal network motifs. In *Conf. on Information Sciences and Systems (CISS)*, pages 1–5, Princeton, NJ, USA, 2012.
- [49] T. Wong, M. Wong, and C. Lui. A precise termination condition of the probabilistic packet marking algorithm. *IEEE Trans. on Dependable and Secure Computing*, 5(1):6–21, 2008.
- [50] Y. Xiang, K. Li, and W. Zhou. Low-rate ddos attacks detection and traceback by using new information metrics. *Information Forensics and Security, IEEE Trans. on*, 6(2):426–437, 2011.
- [51] A. Yaar, A. Perrig, and D. Song. Fit: fast internet traceback. In *Proc. of IEEE INFOCOM Conf.*, pages 1395–1406, Miami, FL, USA, 2005.
- [52] Q. Yan, X. He, and T. Ning. An improved dynamic probabilistic packet marking for ip traceback. *IJCNIS*, 2(2):47–53, 2010.
- [53] M.-H. Yang and M.-C. Yang. Riht: A novel hybrid ip traceback scheme. *Information Forensics and Security, IEEE Trans. on*, 7(2):789–797, 2012.

- [54] G. Yao, J. Bi, and Z. Zhou. Passive ip traceback: capturing the origin of anonymous traffic through network telescopes. In *Proc. of the ACM SIGCOMM Conf.*, pages 413–414, New Delhi, India, 2010.
  
- [55] C.-H. Yeang, L.-C. Huang, and W.-C. Liu. Recurrent structural motifs reflect characteristics of distinct networks. In *IEEE/ACM Int. Conf. on Advances in Social Networks Analysis and Mining (ASONAM)*, pages 551–557, Istanbul, Turkey, 2012.
  
- [56] S. H. Yook, H. Jeong, and A. L. Barabási. Modeling the internet’s large-scale topology. *Proc. of the National Academy of Sciences*, 99(21):13382–13386, 2002.