Improving Stochastic Network Tomographic Models for Attack Detection

Benjamin Sylvester Millar

A thesis submitted for the degree of
Bachelor of Advanced Computing (Honours)
The Australian National University

September 2021

Draft Copy – 3 September 2021

Except where otherwise indicated, this thesis is my own original work.

Benjamin Sylvester Millar
3 September 2021

To my mother Kerrie, my grandparents Edna, Norma, Keith and Victor, and my partner Olivia for all their support and love.

Acknowledgments

Who do you want to thank?

Abstract

Put your abstract here.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation and outline

Network Tomography is the technique of using end-to-end measures to make inferences about that computer network. In this way it is similar to computed axial tomography (CAT) scans in the medical world where x-rays are passed through a patient as a noninvasive method of gaining information pertaining to the interior of the patient. These x-rays are fired from multiple points around the exterior of the patient, they attenuate as they pass through different densities of the tissue and are measured as they exit the body. This process results in a single 2 dimension 'slice' of tissue density in the body being calculated. This is typically repeated over many slices next to one another to give a 3 -dimensional representation.

Network tomography is most analogous to a single one of these slices however instead of using the attenuation of x-rays to infer body tissue density we observe the latency of communication to infer the structure and behaviour of routers within a network. In network science this latency is referred to as a delay and is calculated from the time a given 'packet' or discrete signal takes to traverse the network to its predetermined destination. It should be noted that although in network science there are various forms of signal casting - primarily broadcasting, uni-casting, multi-casting, and any-casting - we will focus on the case of a uni-casted signal. This is as the inclusion of alternative casting methods introduces enough complexity to the analysis that the exploration of tomography under each casting method has spawned its own sub field of research [7].

The primary motivations for network tomography are topology identification [4, 5], general internal state inference [1, 6, 8] and in the case of Boolean tomography, node failure localisation [10, 22]. In this body of work we focus on internal state inference, specifically in the form of identification of abnormal behaviors of network components, potentially caused by a nefarious actor intent on disrupting network behaviour. As such we refer to these induced cases of abnormal behaviour and the offending network components causing these as 'nefarious'. We take this lens as the existence of adversarial settings is a key differentiator between theoretical and real world applications of any technology.

As network tomography is maturing it is beginning to be implemented in many real world settings with support from emerging protocols and platforms such as

Consul [18] and future support in the form of network coding based approaches discussed in [19]. The increasing use of this in real world settings therefore demands research into methods of further validating and optimising the performance of network tomography in these industrial, public and private communication infrastructure settings.

Historical work on uni-cast tomography focuses primarily on networks with an absence of queue buffers, resulting in packet's taking static paths through a network. This assumption was relaxed by Lai and Baker [20] in their work focusing on routing behaviours resulting in stochastic routing networks. Recent work by Barnes [13] has used this approach to introduce nefarious behavior in stochastic settings and subsequently detect this behaviour. In doing this the simulation developed was made more applicable to real world networks.

We aim to build upon this work of nefarious behaviour detection in stochastic environments by relaxing further assumptions in order to better simulate mid-sized complex real world networks such as a home or IoT network. We focus on ensuring methods employed are scalable to far larger networks in hope of maintaining general applicability to large scale real world networking such as that in academic, consumer ISP and commercial data center networks underlying modern cloud infrastructure. The key assumptions under which Barnes based their work are:

1. *End Nodes of the network are switches.*
2. *All packets originate and terminate at switches.*
3. *All routers which are not nefarious behave identically.*
4. *Packets are not dropped when traffic is heavy, instead accumulating in queues of unbound length.*
5. *Background traffic across the network has a constant average intensity.*
6. *All end nodes are equally likely to send packets, and be chosen to receive packets.*
7. *All routing protocols are the same for non-nefarious routers.*
8. *The service time for every packet at the front of the queue in a router is 1 "Time step".*

We focus on the relaxation of 2, 3, 4, 6, 5 and 7 and leave future work to address additional simplifications. These were chosen as assumption 1 allows for a bounded network size as without switches as end nodes we would be forced to instead model all sub-networks which are connected to these switches, and the networks connected to the switches of those sub-networks recursively. This would eventual end in the model representing the observable internet connected to this network, thus being unbounded in size and therefore both impractical and non useful to analyse. We instead maintain this assumption to allow for analysis of arbitrary sub-networks which may be of interest to the typical network administrator, with adjacent networks able to represented a single node with a number of switches connected proportionally to

the typical traffic from that network. Assumption 8 is key to the analysis technique used within the work, the difficulty behind its relaxation is explored in later sections, but the relaxation of this particular assumption is left to further work on the topic.

In the implementation of these complex behaviours resulting from this relaxation we hope to accomplish a primary goal of ensuring the established mechanisms for gaining tomographic inference are robust enough to identify nefarious behaviour in complex real-world systems. Additionally we aim to use this exploration to complete two secondary objectives relating to network tomographic inference of nefarious nodes within a network. Firstly to fix inconclusive results in the work of Barnes relating to the impact of monitor placement algorithms on identifiability of nefarious router sets. Secondly, in the vein of Zhao, Lu, and Wang [21], we lay the framework for the inclusion of alternate attack methods into complex stochastic tomographic models and quantify the effect of these attacks on the power of tomographic inference. The importance of the analysis of tomography accuracy in such adversarial settings is still a fledgling field of research with very few studies on the topic as noted in a compilation of current work in He et al. [8].

1.2 Current Stochastic Models

Current work surrounding network tomographic models identifying nefarious nodes in stochastic networks is led by the work of Barnes [13]. This work falls under the previously mentioned mathematicians approach to tomography and based upon the requirement that the system must be formally mathematically modelable. The network modeling simulation completed as part of that paper consists of 3 distinct sections, the generation of a network, the simulation of packets traversing this network and the compilation of metrics and calculations for the tomographic inference. Over this section we will introduce methods used in this model along with candidate areas considered for extension with the intent of providing more explanation and background on these techniques in §2.

1.2.1 Network generation

The first of the model's sections, referred to onwards as network generation, aims to produce a constrained random undirected graph representing a small to medium sized network of routers and switches. The generated network must contain 4 essential components, routers to direct packets, links between routers for packets to traverse, Switches which emulate connection to a larger external network (i.e. the world wide web) through stochastic production of packets and Monitors a modified switch used in tomographic analysis.

Monitors in the case of this model function as normal switches with regards to packet generation and reception but perform additional recording functionality. Each monitor stores information pertaining to each packet which is generated or received by itself. This stored information is analogous to a traceroute of the packet's path through the network; a list of routers that the packet has passed through. The

monitors also store the total time taken by the packet for it's traversal, as well as the source and destination IP.

Within the graph resulting from the network generation, all edges are undirected and represent links between machines (router, switches or monitors). For simplicity each distinct pair of nodes may only be linked by a single edge, however multiple physical links between a pair of machines occur in the real world, the edge can be considered a virtual aggregation of all of these links, representing their total cumulative throughput. Each node within the graph is a representation of a physical piece of networking hardware, either a router or switch, these are simplified abstractions of their real world analogous, with their key simplifications being those enumerated in the previous section.

The current network generation strategy follows that of the Erdős–Rényi (ER) model; this was introduced in 1959 by Gilbert [30] and later that year revisited in "On Random Graphs I." by the model's titular author pair [31]. This random graph generation is characterised by each node in a graph being connected to each other node with a predefined probability of p, that is for a graph G with n nodes and a connectivity probability p:

$$\textit{where } n > 1 \textit{ and } 0 \leq p \leq 1,\ G = f(n, p)$$

This random graph generation strategy is intuitive in its simplicity however has several problems when used to generate graphs analogous to computer networks. The most prominent shortcomings are in the node degree distribution and presence of so called 'isolated nodes'. A key underlying assumption of the ER model is that each edge between two nodes is equally likely to occur within a graph. The natural consequence of this assumption is that the distribution of node degree's (number of connected edges) within the graph approximates a Poisson distribution [29]. Such random networks are referred to as exponential networks as the probability that a node is connected to n other nodes decreases exponentially as $n \to \infty$.

Complex networks however have not been observed to follow a random pattern but rather that, irrelevant of age, function or scope converge to a similar architecture as shown in Albert, Jeong and Barabási's mapping of the world wide web [28]. This network architecture has been dubbed as scale-free and is characterised by the distribution of node degree following a power-law where the probability of a node having k edges $P(k)$ is proportional to $\frac{1}{kn}$ for a network of n nodes. This property is present in graphs generated using the Barabási–Albert (BA) model, as well as the Watts–Strogatz model; these generation techniques among others are further discussed in §2.

As the network being generated and analyzed continues to increase in size we expect its behaviour and structure to become increasingly complex. Given this complex nature the scale-free property of graph generation is highly desirable for generation of pseudo realistic networks.

1.2.2 Traffic Simulation

The accumulation of all packets sent between each node in the network (referred to as network traffic or simply traffic) and it's simulation is a key aspect of any tomographic model. Intuitively the traffic within a network is generated as a accumulation of all packets from each switch within that network, and the traffic at any single router is determined by the number of paths that pass through it and the number of packets sent along these paths. Given that the traffic simulation is split into discrete time steps of a uniform arbitrary length, we assume that each time step is a period small enough that only a single packet is handled in each step. This has been shown to be binomial distribution [13] over a time window which approaches a Poisson distribution over a large enough number of time steps. From [13], where n denotes the number of time steps, k being the number of packets sent and s being the probability on any given time step that a packet will be sent:

$$\lim_{n\to\infty} \frac{n!}{k!(n-k)!} s^k (1-s)^{n-k} = \frac{s^k e^{-s}}{k!}$$

This distribution of packets being sent is key in the current body of work as it allows for the traffic being sent across a network to be represented as a random variable S with a known distribution and a value of 1 or 0 depending on if a packet is sent or not.

After these packets are sent from switches they are forwarded between routers until they reach their destination as multiple packets may be forwarded to a single router each time step these packets can accumulate in the respective routers' queues, waiting to be forwarded. Given each packet takes a single time step to be processed and forwarded, these queue lengths represent the delay each packet experiences upon traversing a router. Similarly to that of packets, queue lengths and consequently packet delay can be expressed as a random variable Q. Prior work has shown that Q both converges to a steady state over time and, given its dependency on the queue length at the previous time step, is a Markov process [13]. However, Q for each router is a consequence of not only the number of packets sent S, but also the paths these packets take through the network; the routing method used by the network therefore must be scrutinised to utilize a Markov chain model to quantify Q.

For network traffic to be stochastic in nature any routing protocol must be dynamic in nature, else fixed routing tables would be established and only a single path would be taken by a packet between any two switches within the network. Current work uses an abstract implementation of the distance vector routing protocol to achieve this dynamic routing behaviour, with a global controller using Dijkstra's algorithm to compute the shortest distance between any two given nodes and broadcast this information to all components in the network [13]. In this method edge weights for the computation are representative of the number of packets waiting in the queues of each router at the end of that edge as this is analogous to the number of time steps a packet would wait before completing it's traversal of that edge. The

Need a reference for DV

use of a network wide controller in this manner is akin to that of Software Defined Networks (SDNs) where routing logic at the link level is dynamically handled by an SDN controller - we refer the keen reader to the excellent survey by Kreutz et al. [23] for additional information. As most commercial grade networks do not employ SDNs currently and the security concerns surrounding widespread adoption of SDN to control for all traffic on a network moving into the future [24] we highlight the decentralization of this background traffic routing as a key area of work addressed later in this paper.

In the work of Barnes no distinction is made at a routing level between different types of traffic that the router is forwarding, a packet sent by a monitor node that we are able to draw inference from is treated identically to all other packets. We adopt the terminology of Ma in [8] and refer to this as uncontrolled routing (UR), where packets which we are able to observe, as they are sent between monitor nodes, follow the underlying routing behaviour of the network. As routers are able to make distinctions between packets and forward them accordingly, alternative routing of exclusively monitor packets (referred to from here on wards for simplicity as simply routing) is feasible under both normal and SDN conditions. We introduce the alternative forms of routing presented in [8] and outlined in further detail in the following sections, as both key targets for extension of the existing model and methods for quantifying impact of changes on the accuracy of tomographic inference.

Want to put a reference here to our use of Link-State routing and associated proof of queue length and variance stability in the Results

1.2.3 Tomographic Inference

Once packets are collected at each monitor node within the network the distribution of their delays is compared to that expected under different subsets of nefarious routers. The calculation of packet delays is trivial as packets traverse between monitors we are aware of both the time they are sent and the time they arrive. As the path each packet takes through the network is unknown and uncontrollable due to UR the only method of drawing inference is comparison of the observed delay distribution to what we would expect to observe assuming all possible subsets of routers are nefarious. Formally, given a network G and set of nefarious routers R_N we generate $D_G(R_N)$ where $D_x(y)$is a function computing the expected distribution vector of packet delays over a network x given the set of nefarious routers y.

The computation of an expected delay vector is non-trivial as even its approximation is dependent on Q, the number of time steps and the topology of the network. A solution present in [13] uses an agent based method to analytically compute the queue lengths at each router and obtain an estimation of the delay vector under the assumption that the network topology is known a priori and iterated for enough time steps to ensure it has reached a steady state. The resulting delay distribution is then compared to the observed delay distribution using techniques from signal analysis presented by [25] to obtain a correlation metric C where $C(D_x, D_y) = 0$ if D_x has an identical distribution to D_y when both distributions are probability density functions (PDFs) normalised via L2 normalization to yield the Euclidean norm. As this correlation is the only method used to gain inference, this tomographic approach

is only able identify nefarious nodes within a network; sacrificing generality to any other tomographic approach as calculation of all candidate PDFs for every possible link delay or drop configuration to infer the link delay or drop metrics would be computation infeasible.

Show big omega of PDF calculation and comparison over a continuous range of link delay/-drop values

The agent based model used to generate these 'candidate' PDFs was produced under the same assumptions as the network tomographic model. As we are relaxing some of the tomographic models assumptions we anticipate that this agent based generation model will be insufficient to determine the nefarious router configuration resulting in the observed delay distributions. We therefore aim to both relax assumptions in the agent based model similarly to the network model and establish the use of routing techniques other than UR to optimize identification of nefarious routers.

1.2.4 Summary

In this section we have expanded upon the problem of improving existing simulations. We note it serves to treat it instead as 3 separate but related problems of optimisations and extension at each of the previously listed stages. This is as the work done at each stage can be entirely self contained and parsed to another if required, the network can be generated at at earlier point in time, stored and later given to the network traffic simulation, likewise the metrics measures from this simulation can be stored and later used to calculate probabilities of a given router being nefarious.

Optimisation to the code for time complexity is desirable as it allows for larger simulations to be run for more time steps given limited compute resources available. Such extended run time may allow for statistical approximations to converge as seen in section 4.3.1. The simulation of larger networks also allows for the inclusion of real world network topologies such as [15, 16, 17] for analysis, a key requirement for the goal of this body of work. The final artifact of code is presented and made available at [14] in hopes that future work will be able to use this to further expand on this area of work, some specific extensions highlighted in §5.

1.3 Thesis Outline

How many chapters you have? You may have Chapter 2, Chapter 3, Chapter 4, Chapter 5, and Chapter 6.

Chapter 2

Background and Related Work

At the beginning of each chapter, please introduce the motivation and high-level picture of the chapter. You also have to introduce sections in the chapter.

2.1 Motivation

2.2 Related work

The term Network Tomography first came into use in the 1996 paper by Y. Vardi focusing on the estimation of network traffic intensity from individual link data. This estimation is accomplished using a known routing table and frequent measurements of link traffic under an assumed (poisson) distribution. These techniques are lifted directly from related work examining statistical properties of Positron Emission Tomography in the medical field (Used in PET scans) [2]. This allows for the internal state of a network to be reconstructed using only periphery measurements and as such is extremely useful in cases where monitoring of network's where there is no access to internal nodes is required, i.e. subsections of the internet or large GPON's such as the NBN.

Early work in the field such as Vardi's work also touches on the notion of deterministic or markovian routing, specifically under the assumption that fixed routing can be considered as a special case of deterministic routing and as such they both can be solved given the same set of predefined assumptions hold true. The problem of tomography was originally presented as a 'LININPOS' or LINear INverse POSitive problem and only explored as a purely statistical problem; using a more practical lens we would now term this as a form of passive tomography.

Quickly following this initial statistical paper, the study of the emerging field of network tomography (referred to here on wards as simply tomography) split into two related but distinct approaches, that of statisticians/mathematicians and that of computer scientists. Computer scientists further decomposed tomography into passive and active tomography. Passive tomography uses measurements aggregated from observations of all network traffic to calculate properties such as traffic intensity [1, 6] and network topology [3, 4, 5]. The determination of source-destination

traffic intensity is often referred to as traffic matrix or origin destination tomography and focuses on aggregation of internal link measurements to determine network wide traffic [11]. In contrast, network topology identification focuses on forming a best effort approximation of all node-to-node connections based on observed distance metrics. As each of these approaches require access to all network traffic they require a set of edge routers from which this can be observed. Such a set is not always obtainable in real world situations due to hurdles such as traffic anonymization preventing capture of packet sources and the large proportion of edge routers required to be controlled by an observer limiting scalability [12]. Active tomography on the other hand tends to be more applicable to real world systems as it requires less assumed knowledge of the network's state and the observers access to components of the network.

Active tomography, commonly referred to within literature as either Quality of Service (QoS) tomography or network performance tomography [7, 8], can be subdivided into two main approaches of boolean and additive tomography. Each of these approaches is characterised by its representation of internal performance, additionally each approach results in different performance metrics being exposed for evaluation. Boolean tomography represents the internal state of links as an unknown boolean variable, in the conventional case of failure localization this variable corresponds to a "normal" and "failed"' state, as such the inverse problem arises from the success/failure of a source destination path being the logical OR of it's composite paths [9]. In contrast, additive tomography represents the internal state of links as an unknown non-negative values to model non-binary performance metrics - primarily link delay. Given this representation in additive tomography the inverse problem arises from the total delay on a path being the sum of all delays of it's composite paths. Although boolean and additive tomography have many differences in goals and methodologies there are some similarities between them, specifically in the conditions sufficient to allow for inferences to be drawn.

The topological conditions under which inferences are able to be made in both additive and boolean tomography vary depending on routing policy used for monitor probes. An excellent derivation of these conditions can be found in [8] however here we summarise and present these conditions under different routing mechanisms in §2.6. In all cases however, for both additive and link tomography end to end measures are used to infer individual link level performances characteristics of the network.

It should be noted that although all previous work focuses on link metrics, we are able to generalise this to inferring node characteristics by treating each link within a network as a node and vice versa. This is due to a graph

All work up to this point has focused on the notion of deterministic link performance, however in real world networks this assumption is seldom correct.

The investigation of stochastic performance on router links, and consequently routing behaviours, has become increasingly popular in recent years. The use of tomography to draw link level performance inferences in such an environment is termed stochastic network tomography and most current work on the topic, like

that of active tomography, can be split into two subcategories of boolean and non-boolean. Both these techniques seek to identify the distribution of associated metrics according to an unknown parameter θ, the goal of tomography is therefore to estimate θ end to end observations [33]. Boolean stochastic tomography focuses on the packet loss of a network where packet drops are non-deterministically dropped from the network, potentially by an intermittent node or link failure. In contrast, non-boolean stochastic tomography looks to infer information around expected delays on each link, possibly caused by signal congestion or signal handling techniques such as deep packet inspection (DPI) [32]. Both of these tasks are accomplished through the use of Fisher Information Matrices (FIM) with known and controllable routes to develop Maximum Likelihood Estimators (MLEs); the specifics of this technique are covered in detail in §2.5.

Finally, the work of Barnes [13] the use of tomography to infer link level performance in a stochastic system was foregone in favour of the ability to identify 'nefarious' nodes. This was accomplished through the development of an MCMC model to simulate expected queue lengths at nodes given possible configurations of nefarious routers. Nefarious routers in this work are represented as ones which have a probability at any discrete time step of not forwarding a packet to the next router. The delay distributions generated by the MCMC model are then compared to that observed at monitor nodes and the most closely correlated is shown to be a correct prediction of the set of nefarious routers. The primary goal of our work seeks to apply techniques of packet delay estimation in [33] to improve efficacy and efficiency of this nefarious router identification.

2.3 Graph Generation Algorithms

Current work around nefarious router identification in stochastic networks uses numpy's pseudo-random generation against a user defined connectivity parameter to generate edges between nodes. This is analogous to the Erdos-Renyi (ER) generation. Given this work's choice to move to the more performant iGraph module, several ready made random graph generations methods are available including: ER, Random Geometric Graph (GRG), Barabasi-Albert (BA), Watts-Strogatz, Stochastic Block Model(SBM), Preference (and asymmetric preference), multiple Growing Random Game, Recent Degree models and generation techniques with fixed parameters such a given degree sequences or power-law degree distributions [27] . Due to the desire to emulate realistic small-world network's connectivity and topography, the Barabási–Albert model was selected as the most applicable random network generator for this work. This is due to several properties of the model compared to other options. The accurate mimicry of the networks converges to a power law as is observed in real work computer networks, rather than a Poisson distribution as is observed in other more naive network generation algorithms such as the Erdős–Rényi model. The Watts–Strogatz model, although slower in its graph construction, allows for conformity to this power law as well as some of the clustering behaviour observed

in real world networks and as such will also be used.

Although not all random generation techniques produce models analogous to real world networks, for the sake of completeness and to test the robustness each of the ER, BA, SBM, and GRG algorithms are used to evaluate model performance.

2.4 Monitor Placement Algorithms

2.5 Routing Mechanisms

2.6 Markov Chain Monte Carlo

2.7 Parameter Estimation

In this section we frame network tomography and the networks we intend to analyse in a mathematical lens and introduce the fundamental statistical concepts behind our tomographic analysis. We note that a network as we have defined it is composed of only nodes (routers, switch and monitors) and physical uniform links, inferences made about a network are analogous to inferences of nodes and links.

The first of these key concepts is Maximum Likelihood Estimation (MLE) to determine the node and link level parameters which give the highest chance of having observed the given packet delays and losses at monitor nodes. The second is the notion of Fisher Information to quantify both the amount of knowledge we have about the underlying network and the accuracy of our MLE of node and link parameters. We finally summarise the introduced concepts and concretely qualify their use in the field of network tomography.

2.7.1 Maximum Likelihood Estimation

Any complex system, such as a network, can be represented as a suitably complex probabilistic model which takes in a set of parameters $\theta \in \Theta$ where Θ denotes the parameter space of all possible values of θ and generates results $O \in \mathbb{R}$ according to these parameters or more formally:

$$f(\theta) = O$$

As this function is probabilistic we note that the set O is only an observed sample distribution from an underlying population. In network tomography we can view these θ as network properties or more productively - as a network is composed only of links and nodes - the link and node level information which we are looking to infer from our analysis. We therefore can invert this system and instead pose it as $L_n(\theta|O)$ where L_N ndenotes the likelihood of observing O given a model governed by the parameters θ. We then want to determine the most likely set of parameters $\hat{\theta}$ which are could have been used generate our observations, by convention this is posed as $\hat{\theta} = argmax_{\theta \in \Theta} L_n(\theta|\Theta)$.

2.7.2 Fisher Information Matrices

2.8 Summary

Summary what you discussed in this chapter, and mention the story in next chapter. Readers should roughly understand what your thesis takes about by only reading words at the beginning and the end (Summary) of each chapter.

Chapter 3

Design and Implementation

Same as the last chapter, introduce the motivation and the high-level picture to readers, and introduce the sections in this chapter.

Chapter 4

Methodology

Chapter 5

Results

5.1 Direct Cost

Here is the example to show how to include a figure. Figure **??** includes two subfigures (Figure **??**, and Figure **??**);

5.2 Summary

Chapter 6

Conclusion

Summary your thesis and discuss what you are going to do in the future in Section 6.1.

6.1 Future Work

Good luck.

Bibliography

Albert, R. and Barabási, A.-L., 2002. Statistical mechanics of complex networks. *Reviews of Modern Physics*, 74, 1 (2002), 47–97. doi:10.1103/revmodphys.74.47. https://dx.doi.org/10.1103/revmodphys.74.47. Publisher: American Physical Society (APS).

Albert, R.; Jeong, H.; and Barabási, A.-L., 1999. Diameter of the World-Wide Web. *Nature*, 401, 6749 (1999), 130–131. doi:10.1038/43601. https://dx.doi.org/10.1038/43601. Publisher: Springer Science and Business Media LLC.

ALBERT-LÁSZLÓ, B. and BONABEAU, E., 2003. Scale-Free Networks. *Scientific American*, 288, 5 (May 2003), 60–69. doi:10.2307/26060284. https://dx.doi.org/10.2307/26060284.

Arrigoni, V.; Bartolini, N.; Massini, A.; and Trombetti, F., 2021. Static and Dynamic Failure Localization through Progressive Network Tomography. *arXiv pre-print server*, (Mar. 2021). https://arxiv.org/abs/2103.17221.

Balasubramonian, R.; Dwarkadas, S.; and Albonesi, D. Reducing the complexity of the register file in dynamic superscalar processors. IEEE Comput. Soc. doi:10.1109/micro.2001.991122. https://dx.doi.org/10.1109/micro.2001.991122.

Barabási, A.-L., 2009. Scale-Free Networks: A Decade and Beyond. *Science*, 325, 5939 (2009), 412–413. doi:10.1126/science.1173299. https://dx.doi.org/10.1126/science.1173299. Publisher: American Association for the Advancement of Science (AAAS).

Barnes, A., 2020. *Stochastic Network Tomography: Inferring Network Properties from Limited Monitor Data*. Ph.D. thesis, Australian National University, Canberra.

Bertotti, M. L. and Modanese, G., 2019. The configuration model for Barabasi-Albert networks. *Applied Network Science*, 4, 1 (2019). doi:10.1007/s41109-019-0152-1. https://dx.doi.org/10.1007/s41109-019-0152-1. Publisher: Springer Science and Business Media LLC.

Bolot, J.-C., 1993. End-to-end packet delay and loss behavior in the internet. ACM Press. doi:10.1145/166237.166265. https://dx.doi.org/10.1145/166237.166265.

Cao, J.; Davis, D.; Vander Wiel, S.; and Yu, B., 2000. Time-Varying Network Tomography: Router Link Data. *Journal of the American Statistical Association*, 95, 452 (2000), 1063–1075. doi:10.1080/01621459.2000.10474303. https://dx.doi.org/10.1080/01621459.2000.10474303. Publisher: Informa UK Limited.

Cascares; Duffield; Horowitz; and Towsley, 1999. Multicast-based inference of network-internal loss characteristics. *IEEE Transactions on Information Theory*, 45, 7 (1999), 2462–2480. doi:10.1109/18.796384. https://dx.doi.org/10.1109/18.796384. Publisher: Institute of Electrical and Electronics Engineers (IEEE).

Chiu, C.-C. and He, T., 2021. Stealthy DGoS Attack Against Network Tomography: The Role of Active Measurements. *IEEE Transactions on Network Science and Engineering*, 8, 2 (2021), 1745–1758. doi:10.1109/tnse.2021.3070990. https://dx.doi.org/10.1109/tnse.2021.3070990. Publisher: Institute of Electrical and Electronics Engineers (IEEE).

Coates, A.; Hero Iii, A.; Nowak, R.; and Bin Yu, 2002. Internet tomography. *IEEE Signal Processing Magazine*, 19, 3 (2002), 47–65. doi:10.1109/79.998081. https://dx.doi.org/10.1109/79.998081. Publisher: Institute of Electrical and Electronics Engineers (IEEE).

Coates, M. and Nowak, R. Network tomography for internal delay estimation. IEEE. doi:10.1109/icassp.2001.940573. https://dx.doi.org/10.1109/icassp.2001.940573.

Dong, W.; Gao, Y.; Wu, W.; Bu, J.; Chen, C.; and Li, X.-Y., 2017. Optimal Monitor Assignment for Preferential Link Tomography in Communication Networks. *IEEE/ACM Transactions on Networking*, 25, 1 (2017), 210–223. doi:10.1109/tnet.2016.2581176. https://dx.doi.org/10.1109/tnet.2016.2581176. Publisher: Institute of Electrical and Electronics Engineers (IEEE).

Duan, Q.; Cai, W.; and Tian, G., 2009. A Simple Graph-structure Network Tomography Topology Identification Method. IEEE. doi:10.1109/jcai.2009.141. https://dx.doi.org/10.1109/jcai.2009.141.

Duffield, N., 2006. Network Tomography of Binary Network Performance Characteristics. *IEEE Transactions on Information Theory*, 52, 12 (2006), 5373–5388. doi:10.1109/tit.2006.885460. https://dx.doi.org/10.1109/tit.2006.885460. Publisher: Institute of Electrical and Electronics Engineers (IEEE).

El-Maghraby, R. T.; Abd Elazim, N. M.; and Bahaa-Eldin, A. M., 2017. A survey on deep packet inspection. IEEE. doi:10.1109/icces.2017.8275301. https://dx.doi.org/10.1109/icces.2017.8275301.

E.N, G., 1961. Random Plane Networks. *Journal of the Society for Industrial and Applied Mathematics*, 9, 4 (1961), 533–543. doi:10.2307/2098879. https://dx.doi.org/10.2307/2098879.

Ghita, D.; Karakus, C.; Argyraki, K.; and Thiran, P., 2011. Shifting network tomography toward a practical goal. ACM Press. doi:10.1145/2079296.2079320. https://dx.doi.org/10.1145/2079296.2079320.

Gilbert, E. N., 1959. Random Graphs. *The Annals of Mathematical Statistics*, 30, 4 (1959), 1141–1144. doi:10.1214/aoms/1177706098. https://dx.doi.org/10.1214/aoms/1177706098. Publisher: Institute of Mathematical Statistics.

Hailiang, L.; Guangmin, H.; Feng, Q.; and Zhihao, Y., 2009. Network Topology Inference Based on Traceroute and Tomography. IEEE. doi:10.1109/cmc.2009.214. https://dx.doi.org/10.1109/cmc.2009.214.

He, T.; Liu, C.; Swami, A.; Towsley, D.; Salonidis, T.; Bejan, A. I.; and Yu, P., 2015. Fisher Information-based Experiment Design for Network Tomography. *ACM SIGMETRICS Performance Evaluation Review*, 43, 1 (2015), 389–402. doi:10.1145/2796314.2745862. https://dx.doi.org/10.1145/2796314.2745862. Publisher: Association for Computing Machinery (ACM).

Horton, J. D. and López-Ortiz, A., 2003. On the number of distributed measurement points for network tomography. ACM Press. doi:10.1145/948205.948231. https://dx.doi.org/10.1145/948205.948231.

Hou, T.; Qu, Z.; Wang, T.; Lu, Z.; and Liu, Y., 2020. ProTO: Proactive Topology Obfuscation Against Adversarial Network Topology Inference. IEEE. doi:10.1109/infocom41043.2020.9155255. https://dx.doi.org/10.1109/infocom41043.2020.9155255.

Huang, Y.; Feamster, N.; and Teixeira, R., 2008. Practical issues with using network tomography for fault diagnosis. *ACM SIGCOMM Computer Communication Review*, 38, 5 (2008), 53–58. doi:10.1145/1452335.1452343. https://dx.doi.org/10.1145/1452335.1452343. Publisher: Association for Computing Machinery (ACM).

Kakkavas, G.; Gkatzioura, D.; Karyotis, V.; and Papavassiliou, S., 2020. A Review of Advanced Algebraic Approaches Enabling Network Tomography for Future Network Infrastructures. *Future Internet*, 12, 2 (2020), 20. doi:10.3390/fi12020020. https://dx.doi.org/10.3390/fi12020020. Publisher: MDPI AG.

Kreutz, D.; Ramos, F. M. V.; Esteves Verissimo, P.; Esteve Rothenberg, C.; Azodolmolky, S.; and Uhlig, S., 2015. Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE*, 103, 1 (2015), 14–76. doi:10.1109/jproc.2014.2371999. https://dx.doi.org/10.1109/jproc.2014.2371999. Publisher: Institute of Electrical and Electronics Engineers (IEEE).

Kumar, S.; Turner, J.; and Williams, J., 2006. Advanced algorithms for fast and scalable deep packet inspection. ACM Press. doi:10.1145/1185347.1185359. https://dx.doi.org/10.1145/1185347.1185359.

Ma, L.; He, T.; Kin; Swami, A.; and Towsley, D., 2020. Link Identifiability with Two Monitors: Proof of Selected Theorems. *arXiv pre-print server*, (Dec. 2020). https://arxiv.org/abs/2012.09972.

Ma, L.; He, T.; Leung, K. K.; Towsley, D.; and Swami, A., 2013. Efficient Identification of Additive Link Metrics via Network Tomography. IEEE. doi:10.1109/icdcs.2013.24. https://dx.doi.org/10.1109/icdcs.2013.24.

Ma, L.; He, T.; Swami, A.; Towsley, D.; and Leung, K. K., 2015. On optimal monitor placement for localizing node failures via network tomography. *Performance Evaluation*, 91 (2015), 16–37. doi:10.1016/j.peva.2015.06.003. https://dx.doi.org/10.1016/j.peva.2015.06.003. Publisher: Elsevier BV.

Magnoux, V. and Ozell, B., 2021. GPU-friendly data structures for real time simulation. *Advanced Modeling and Simulation in Engineering Sciences*, 8, 1 (2021). doi:10.1186/s40323-021-00192-7. https://dx.doi.org/10.1186/s40323-021-00192-7. Publisher: Springer Science and Business Media LLC.

Medina, A.; Lakhina, A.; Matta, I.; and Byers, J. BRITE: an approach to universal topology generation. IEEE Comput. Soc. doi:10.1109/mascot.2001.948886. https://dx.doi.org/10.1109/mascot.2001.948886.

Meng-Fu Shih and Hero, A. Unicast inference of network link delay distributions from edge measurements. IEEE. doi:10.1109/icassp.2001.940576. https://dx.doi.org/10.1109/icassp.2001.940576.

Morrison, A.; Mehring, C.; Geisel, T.; Aertsen, A.; and Diesmann, M., 2005. Advancing the Boundaries of High-Connectivity Network Simulation with Distributed Computing. *Neural Computation*, 17, 8 (2005), 1776–1801. doi:10.1162/0899766054026648. https://dx.doi.org/10.1162/0899766054026648. Publisher: MIT Press - Journals.

Nguyen, H. X. and Thiran, P., 2007. The Boolean Solution to the Congested IP Link Location Problem: Theory and Practice. IEEE. doi:10.1109/infcom.2007.245. https://dx.doi.org/10.1109/infcom.2007.245.

Qian Chen; Hyunseok Chang; Govindan, R.; and Jamin, S. The origin of power laws in Internet topologies revisited. IEEE. doi:10.1109/infcom.2002.1019306. https://dx.doi.org/10.1109/infcom.2002.1019306.

Qiao, Y.; Jiao, J.; Cui, X.; and Rao, Y., 2020. Robust Loss Inference in the Presence of Noisy Measurements and Hidden Fault Diagnosis. *IEEE/ACM Transactions on Networking*, 28, 1 (2020), 43–56. doi:10.1109/tnet.2019.2948818. https://dx.doi.org/10.1109/tnet.2019.2948818. Publisher: Institute of Electrical and Electronics Engineers (IEEE).

Rabbat, M.; Nowak, R.; and Coates, M. Multiple source, multiple destination network tomography. IEEE. doi:10.1109/infcom.2004.1354575. https://dx.doi.org/10.1109/infcom.2004.1354575.

Tabatabaeimehr, F.; Ruiz, M.; Liu, Y.; Chen, X.; Proietti, R.; Yoo, S. J. B.; and Velasco, L., 2021. Cooperative Learning for Disaggregated Delay Modeling in Multidomain Networks. *IEEE Transactions on Network and Service Management*, (2021), 1–1. doi:10.1109/tnsm.2021.3077736. https://dx.doi.org/10.1109/tnsm.2021.3077736. Publisher: Institute of Electrical and Electronics Engineers (IEEE).

Tagyo, R.; Ikegami, D.; and Kawahara, R., 2021. Network Tomography Using Routing Probability for Undeterministic Routing. *IEICE Transactions on Communications*, E104.B, 7 (2021), 837–848. doi:10.1587/transcom.2020ebp3149. https://dx.doi.org/10.1587/transcom.2020ebp3149. Publisher: Institute of Electronics, Information and Communications Engineers (IEICE).

Tebaldi, C. and West, M., 1998. Bayesian Inference on Network Traffic Using Link Count Data. *Journal of the American Statistical Association*, 93, 442 (1998), 557–573. doi:10.1080/01621459.1998.10473707. https://dx.doi.org/10.1080/01621459.1998.10473707. Publisher: Informa UK Limited.

Thoppe, G.; Borkar, V.; and Manjunath, D., 2014. A stochastic Kaczmarz algorithm for network tomography. *Automatica*, 50, 3 (2014), 910–914. doi:10.1016/j.automatica.2013.12.016. https://dx.doi.org/10.1016/j.automatica.2013.12.016. Publisher: Elsevier BV.

Tsang, Y.; Coates, M.; and Nowak, R. Passive network tomography using EM algorithms. IEEE. doi:10.1109/icassp.2001.941208. https://dx.doi.org/10.1109/icassp.2001.941208.

Van Ravenzwaaij, D.; Cassey, P.; and Brown, S. D., 2018. A simple introduction to Markov Chain Monte–Carlo sampling. *Psychonomic Bulletin & Review*, 25, 1 (2018), 143–154. doi:10.3758/s13423-016-1015-8. https://dx.doi.org/10.3758/s13423-016-1015-8. Publisher: Springer Science and Business Media LLC.

Vardi, Y.; Shepp, L. A.; and Kaufman, L., 1985. A Statistical Model for Positron Emission Tomography. 80, 389 (1985), 8. doi:10.2307/2288030. https://dx.doi.org/10.2307/2288030. Publisher: JSTOR.

Wandong, C.; Ye, Y.; and Yongju, L., 2011. Research on Network Tomography Measurement Technique. In *Stochastic Optimization - Seeing the Optimal for the Uncertain*. InTech. doi:10.5772/15335. https://dx.doi.org/10.5772/15335. Journal Abbreviation: Stochastic Optimization - Seeing the Optimal for the Uncertain.

Yao, H.; Jaggi, S.; and Chen, M., 2012. Passive Network Tomography for Erroneous Networks: A Network Coding Approach. *IEEE Transactions on Information Theory*, 58, 9 (2012), 5922–5940. doi:10.1109/tit.2012.2204532. https://dx.doi.org/10.1109/tit.2012.2204532. Publisher: Institute of Electrical and Electronics Engineers (IEEE).

Zhang, R.; Li, Y.; and Li, X., 2014. Topology Inference With Network Tomography Based on t-Test. *IEEE Communications Letters*, 18, 6 (2014), 921–924. doi:10.1109/lcomm.2014.2317743. https://dx.doi.org/10.1109/lcomm.2014.2317743. Publisher: Institute of Electrical and Electronics Engineers (IEEE).

Zhao, S.; Lu, Z.; and Wang, C., 2017. When Seeing Isn't Believing: On Feasibility and Detectability of Scapegoating in Network Tomography. IEEE. doi:10.1109/icdcs.2017.23. https://dx.doi.org/10.1109/icdcs.2017.23.

Zhao, S.; Lu, Z.; and Wang, C., 2020. Measurement Integrity Attacks against Network Tomography: Feasibility and Defense. *IEEE Transactions on Dependable and Secure Computing*, (2020), 1–1. doi:10.1109/tdsc.2019.2958934. https://dx.doi.org/10.1109/tdsc.2019.2958934. Publisher: Institute of Electrical and Electronics Engineers (IEEE).