Approach to Failures in Complex Networks and Possible Interventions

विद्या वाचस्पति की
उपाधि की अपेक्षाओं की आंशिक पूर्ति में प्रस्तुत शोध प्रबंध

A thesis submitted in partial fulfillment of the requirements of the degree of Doctor of Philosophy

द्वारा / By
शौनक रॉय / Shaunak Roy
पंजीकरण सं. / Registration No.: 20172035

शोध प्रबंध पर्यवेक्षक / Thesis Supervisor:
प्रो. एम. एस. संथानम / Prof. M. S. Santhanam



भारतीय विज्ञान शिक्षा एवं अनुसंधान संस्थान पुणे

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH PUNE

2026

List of Publications

1. Roy, S., Kishore, V., & Santhanam, M. S. (2026). "Approach to network failure due to intrinsic fluctuations." *Physical Review E*, **113**, L062302.

   DOI: 10.1103/PhysRevE.113.L062302

2. Roy, S., Kishore, V., & Santhanam, M. S. Effect of repair on flux-driven networks. *Manuscript in preparation.*

3. Roy, S., Kishore, V., & Santhanam, M. S. Path to failure: a study from structural perspective on flux-driven networks. *Manuscript in preparation.*

Certificate

Certified that the work incorporated in the thesis entitled "*Approach to failures in complex networks and possible interventions*", submitted by *Shaunak Roy,* was carried out by the candidate under my supervision. The work presented here or any part of it has not been included in any other thesis submitted previously for the award of any degree or diploma from any other university or institution.



Date: March 24, 2026

Prof. M S Santhanam

Thesis Supervisor

Declaration

Name of the student: Shaunak Roy

Reg. No.: 20172035

Thesis Supervisor: Prof. M. S. Santhanam

Department: Physics

Date of joining program: 01/08/2017

Date of Pre-Synopsis Seminar: 11/09/2025

Title of Thesis: Approach to failures in complex networks and possible interventions

I declare that this written submission represents my idea in my own words and where others' ideas have been included; I have adequately cited and referenced the original sources. I declare that I have acknowledged collaborative work and discussions wherever such work has been included. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

The work reported in this thesis is the original work done by me under the guidance of

Prof. M. S. Santhanam.

Date: 24 March 2026



Shaunak Roy

Dedicated to Bharat——the eternal and ever-embracing motherland, whose timeless spirit inspires the pursuit of knowledge and the service of all life.

Acknowledgements

"This thesis represents a journey of learning not only how to do research, but also how to grow through a range of experiences beyond the final destination."

First and foremost, I would like to express my sincere gratitude to my PhD supervisor, Prof. M. S. Santhanam, for his constant guidance, encouragement, and support throughout my doctoral journey. His insights and perspective have deeply influenced my approach to research. I am especially grateful for the complete intellectual freedom he afforded me during my PhD, allowing me to explore ideas independently while providing timely guidance when needed.

I would also like to thank my co-author, Dr. Vimal Kishore, for valuable discussions and collaborations that significantly contributed to this work.

I am grateful to my RAC members: Prof. Arijit Bhattacharyay and Prof. Sreejith G. J. for their constructive feedback and guidance at various stages of my PhD, and to the Physics staff at IISER Pune for their administrative and technical support.

I gratefully acknowledge the National Supercomputing Mission for providing access to the computing resources of PARAM Brahma at IISER Pune. This facility is implemented by C-DAC and supported by the Ministry of Electronics and Information Technology (MeitY) and the Department of Science and Technology (DST), Government of India. I also acknowledge the use of the computing facilities available at IISER Pune, which were instrumental in carrying out this research.

I gratefully acknowledge the Dr. V. S. Patankar Physics Endowment Fund for its support.

Finally, I would like to thank IISER Pune for providing me with the opportunity and institutional support to conduct this research.

I would also like to acknowledge my colleagues, classmates, and friends for creating a supportive and intellectually stimulating environment. Their discussions, encouragement, and companionship made this journey enriching and enjoyable. I am especially grateful to my office mate, Bharathi, who has been a constant companion through countless discussions, basketball games, and tea breaks, making everyday academic life more engaging and memorable.

I would also like to thank my basketball friends—Anupam, Anant, and Salam—for the camaraderie and refreshing moments on and off the court, which provided a much-needed balance during my PhD. I am grateful to Sarvottam for his insightful discussions and valuable assistance with coding, which greatly contributed to this work.

I would also like to thank Aakash, my roommate, and Mayank, Ritam, Ajit for their constant support and companionship throughout this journey.

Finally, I express my deepest gratitude to my family and my wife for their unwavering support, patience, and encouragement throughout this journey. Their belief in me has been my greatest strength.

Shaunak Roy
IISER Pune

Abstract

Modern infrastructure systems — power grids, communication networks, transportation systems, and financial markets — are routinely operated near their functional limits, making them susceptible to large-scale failure even in the absence of external perturbations. While existing literature has focused predominantly on failure induced by targeted attacks or random node removal, this thesis investigates a comparatively underexplored mechanism: network failure driven entirely by intrinsic stochastic fluctuations in node flux.

Flux transport is modeled using multiple independent random walkers on a network, where the instantaneous walker count at each node constitutes a stochastic load. An extreme event is declared when this load exceeds a degree-dependent threshold, defined as a fixed number of standard deviations above the mean. When such an event occurs, the affected node is permanently disabled and its load redistributed to neighboring nodes, potentially triggering further failures. The central question addressed is how this purely internal mechanism drives a network from normal operation to complete collapse.

The principal finding of this thesis is that network failure induced by intrinsic fluctuations is not abrupt or unpredictable, but unfolds through three universally observable regimes, characterized using the capacity-to-load ratio η as an order parameter. In the *independent failure regime*, extreme events are rare and spatially uncorrelated; the network sustains near-normal operation. As η decreases, the system enters the *cascade failure regime*, where individual node failures redistribute load onto neighbors, triggering correlated bursts of secondary failures. Finally, the *overload regime* marks the terminal phase, in which residual network capacity falls so far below total load that all remaining nodes fail within one or two time steps. This three-regime structure is derived analytically for the all-to-all network and confirmed numerically across Erdős–Rényi, Barabási–Albert, Watts–Strogatz, square-lattice, and real-world flight networks, establishing its universality across topological classes.

Recurrence-time statistics reveal that the mean inter-event time at a node decreases sharply as the network degrades, and its collapse below unity provides a natural, computable early-warning signal for the onset of the cascade regime.

The thesis further investigates the effect of delayed repair dynamics. A nonlinear delay differential equation is derived that captures the competition between state-dependent failure and recovery, predicting a critical repair delay τ_R^* that separates a survival phase from irreversible collapse — a transition structurally analogous to percolation thresholds in classical network robustness theory. Crucially, slow repair initiated during the independent regime is both sufficient and resource-efficient; once the cascade is established, repair demands escalate sharply and become effectively infeasible in the overload regime. Analysis of failure-time rankings across scale-free and Apollonian networks further identifies a structural early-warning signature: low-degree nodes fail first, but cascade onset is marked by the failure of intermediate-degree nodes, providing an observable, real-time indicator of impending systemic collapse.

Together, these results challenge the prevailing paradigm that network resilience requires only protection against external shocks. Internal fluctuations, ubiquitous in real infrastructure systems, are alone sufficient to drive progressive and irreversible network failure. The capacity-to-load ratio η emerges as a practical, topology-independent diagnostic for real-time health monitoring, and the identified repair window and early-warning signatures provide actionable principles for designing resilient networked systems.

Contents

Acknowledgements ii

Abstract iv

1 Introduction 1
- 1.1 Motivation . . . 1
- 1.2 Overview of Complex Networks . . . 4

2 Dynamical Processes on Networks 20
- 2.1 Introduction . . . 20
- 2.2 Mathematical Representation of Network Dynamics . . . 21
- 2.3 Percolation and Network Resilience . . . 22
- 2.4 Epidemic Spreading . . . 23
- 2.5 Synchronisation . . . 26
- 2.6 Social Dynamics and Opinion Formation . . . 28
- 2.7 Diffusion and Random Walk Processes . . . 29
- 2.8 Random Walk Flux Dynamics and Extreme Events . . . 30
- 2.9 Extreme Value Theory . . . 33
- 2.10 Conclusion . . . 40

3 Network Failure Induced by Intrinsic Fluctuations 42
- 3.1 Introduction . . . 42
- 3.2 Extreme Events on Complex Networks . . . 45
- 3.3 Extreme events and network failure . . . 46
- 3.4 Approach to network failure . . . 50
- 3.5 Summary . . . 62

4 Repair on Networks 64
- 4.1 Theoretical Foundations . . . 64
- 4.2 Failure Mechanisms . . . 65
- 4.3 Conceptual Framework for Repair . . . 65
- 4.4 Local Repair Mechanisms . . . 66

4.5 Global Repair Strategies . . . 67
4.6 Stochastic Models of Repair . . . 67
4.7 Cascading Failures and Repair . . . 68
4.8 Topology-Dependent Repair Efficiency . . . 68
4.9 Adaptive and Co-evolving Networks . . . 69
4.10 Metrics for Repair Efficiency and Resilience . . . 69
4.11 Effect of Repair on Flux-Driven Networks . . . 69
4.12 Recurrence Time and the Window for Repair . . . 71
4.13 Critical Repair Delay and the Survival Transition . . . 72
4.14 Structural Signatures of Failure . . . 75
4.15 Summary . . . 77

5 Conclusion **79**
5.1 Summary of Results . . . 79
5.2 Limitations and Future Directions . . . 80

Bibliography **82**

Chapter 1

Introduction

1.1 Motivation

Modern society rests on a web of interconnected systems: power grids, the Internet, transportation networks, financial markets, and supply chains. These infrastructures have been engineered over decades to be efficient and reliable, yet they share a striking vulnerability: they routinely operate close to their functional limits, and even modest disturbances can trigger consequences far larger than the initiating event [1, 2]. The 2003 North American blackout, which began from a software bug and a few tripped lines in Ohio and ultimately left roughly 55 million people without power [3], is a vivid illustration of how interconnection, while enabling efficiency, simultaneously creates channels for failure propagation. The 2012 Indian power grid blackout stands as one of the largest cascading failures in modern infrastructure systems, affecting over 600 million people across multiple regions[4]. The disturbance was not triggered by a single fault but emerged from a combination of systemic stresses, including heavy power overdrawal in the Northern region, transmission constraints, and weakened reliability margins. When key transmission lines tripped due to overload and power swings, the system rapidly lost stability. This led to a sharp decline in grid frequency, triggering generator protections and widespread outages. As shown in Fig. 1.1, the system frequency remains close to nominal values before undergoing a rapid collapse, characteristic of a cascading failure. A critical insight from the event is the presence of poorly damped oscillatory modes and inadequate real-time control, which left the system vulnerable to disturbances. The failure highlights how large-scale power grids behave as complex networks,

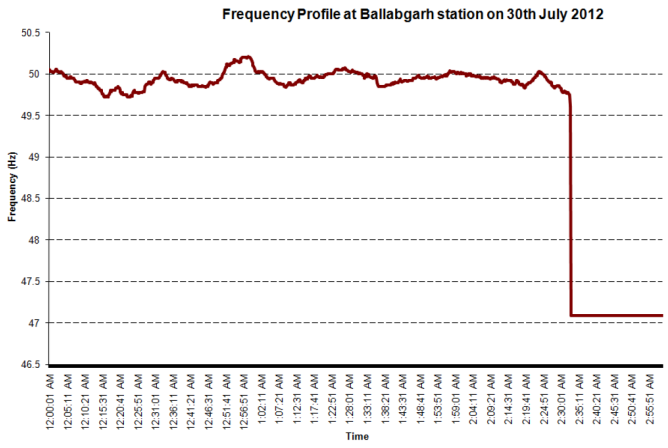


Figure 1.1: Frequency profile at Ballabgarh substation on 30th July 2012 showing a sudden collapse from nominal $\sim$ 50 Hz to $\sim$ 47.1 Hz around 02:33 hours, indicating a cascading failure in the Northern grid. The sharp drop reflects loss of generation-load balance and subsequent system instability.Figure taken from [4]

where local disruptions can propagate nonlinearly into global collapse. It underscores the importance of grid discipline, robust protection mechanisms, and enhanced monitoring to prevent such extreme events.

Historically, research on network failure has concentrated on *external shocks*, deliberate targeted attacks, natural disasters, or sudden demand surges [5, 6, 7]. This body of work established the now-classical picture that scale-free networks, though resilient to random removal of nodes, are highly susceptible to targeted removal of their most connected hubs [5]. However, an equally important yet comparatively underexplored source of failure is *intrinsic fluctuations* - disturbances that arise not from any external agent but from the system's own stochastic dynamics. Even when a network is structurally intact and operating normally, the random nature of the processes occurring on it : diffusion, transport, load fluctuations, can occasionally concentrate enough stress at a single node or edge to push it beyond its operational threshold. Such rare but severe occurrences are termed *extreme events* [8, 9, 10].

What makes extreme events particularly interesting in the context of networks is that they do not occur uniformly across the system. The structural heterogeneity of a network - the fact that different nodes have vastly different numbers of connections - means that fluctuations are amplified unevenly. Counterintuitively, it is often the *low-degree* nodes, those with few connections, that are most susceptible to extreme events, rather than the highly connected hubs [8, 11]. This structural selectivity has deep consequences for failure propagation: a

local extreme event at a vulnerable node can trigger a cascade that spreads through the network, potentially causing a global breakdown [12, 13].

This thesis is driven by the question of how such *internally generated* fluctuations lead to system-wide breakdowns. A key observation motivating this work is that heterogeneity in network topology does not merely create inequality among nodes, it actively shapes the pathways through which failure spreads [14]. Understanding these pathways raises several fundamental questions that this thesis aims to address:

- Can large-scale network failure emerge purely from internal dynamics, without any external attack or perturbation?
- Which structural features of a network determine which nodes are most vulnerable?
- Are there universal statistical signatures that precede failure and could serve as early-warning indicators?
- How do networks recover after failure, and what repair strategies are most efficient?

A further motivation comes from the recognized limitations of current resilience strategies. Much of the existing literature frames resilience as a property to be engineered into a network's topology - through redundant links, increased capacity, or targeted hardening of critical nodes [15, 16]. While these approaches are valuable, they are insufficient on their own: real systems are dynamic, operate under resource constraints, and cannot always prevent failure. This reality shifts the emphasis from *robustness* alone toward a broader notion of *resilience* that encompasses not only resistance to failure but also the ability to detect impending failure and to recover efficiently once failure has occurred [14].

The interplay between failure and repair introduces a rich dynamical framework. Failures do not happen in isolation; they unfold as part of an evolving process in which damaged components may be progressively restored, the network topology changes, and the system either recovers to functionality or descends into complete collapse [13, 17]. Studying this process in the context of intrinsic fluctuations leads naturally to models that can identify the conditions under which recovery is possible and the strategies that minimize the cost of restoration.

A unifying conceptual thread running through this thesis is the idea of *approaching failure*, viewing network collapse not as a sudden unpredictable event but as the culmination of a

gradual process with detectable precursors. This perspective, well established in the study of critical transitions in dynamical systems [14, 18], suggests that systems approaching a tipping point exhibit characteristic signatures such as increasing variance, slowing recovery from small perturbations, and growing spatial correlations. Identifying analogous precursors in networked systems is a central goal of this work, and has direct practical value for designing early-warning systems that can anticipate and mitigate large-scale breakdowns [19].

From a broader scientific perspective, this thesis sits at the intersection of statistical physics, nonlinear dynamics, and network science. It extends the classical theory of extreme value statistics [20] from low-dimensional settings to the high-dimensional, topology-dependent context of complex networks, where interactions and structure play decisive roles [8, 10, 21]. In doing so, it complements and challenges the conventional narrative that emphasizes external drivers of failure, highlighting instead the fundamental role of complexity and internal dynamics as sources of instability.

1.2 Overview of Complex Networks

1.2.1 Introduction

The study of complex networks has become one of the most active research areas in modern science, not because networks are a new concept, but because the tools to study them at scale, large empirical datasets and powerful computational methods, became widely available only in the last few decades [2, 22]. At its core, network science is concerned with representing and understanding systems whose behavior emerges from the *pattern* of interactions among their constituent parts, rather than from the parts themselves.

The range of systems that can be fruitfully modeled as networks is remarkable. In biology, metabolic networks capture chemical reactions within cells, protein interaction networks map functional relationships between proteins, and neural networks encode synaptic connections in the brain [23, 22]. In technology, the Internet links millions of routers through fiber-optic cables, the power grid connects generators and consumers through transmission lines [24, 25], and the World Wide Web is a directed graph of web pages linked by hyperlinks. In society, co-authorship networks link scientists who have published together, and friendship networks map social ties among individuals. Despite their surface differences, all of these systems share structural and dynamical properties that make a unified theoretical treatment both possible and productive [2].

Formally, a network is represented as a graph

$$G = (V, E), \tag{1.1}$$

where V is the set of *nodes* (also called vertices), representing the system's components, and $E \subseteq V \times V$ is the set of *edges* (also called links), representing the interactions between them. We denote the number of nodes as $N = |V|$ and the number of edges as $M = |E|$. The network is fully described by specifying which pairs of nodes are connected, and in the weighted or directed cases, by additional attributes on the edges. We focus primarily on *undirected, unweighted simple graphs*, meaning that edges carry no direction or weight, and no node has a self-loop or more than one edge to the same neighbor.

What distinguishes complex networks from simple regular graphs (like a lattice) or purely random ones (like an Erdős–Rényi graph) is the presence of *nontrivial* structural features: heterogeneous degree distributions, high clustering, short path lengths, and modular organization [23, 22]. These features are not incidental; they directly govern how processes — disease spread, information flow, load distribution, failure cascades — unfold on the network [13, 14]. This is why understanding network structure is a prerequisite for understanding network dynamics, and why this chapter is devoted entirely to building that structural foundation before we turn to dynamics in the chapters that follow.

1.2.2 Historical Background

The intellectual roots of network science extend back to the eighteenth century. The starting point is conventionally taken to be Leonhard Euler's 1736 solution to the *Seven Bridges of Königsberg* problem. The question was whether one could walk through the city of Königsberg crossing each of its seven bridges exactly once. Euler showed that no such walk was possible by representing the land masses as nodes and the bridges as edges, and proving that a traversal visiting every edge exactly once (now called an *Eulerian path*) requires that all but at most two nodes have even degree. This elegant argument inaugurated graph theory, and the language Euler introduced - nodes, edges, paths - remains the foundation of network science today.

For nearly two centuries, the mathematical study of graphs remained primarily a tool of pure combinatorics and topology. The next major conceptual leap came in the 1950s and 1960s, when Paul Erdős and Alfréd Rényi introduced the *random graph* [26, 27]. In their model, a

graph on N nodes is formed by connecting each pair of nodes independently with probability p. They proved a series of striking results about the structure of such graphs as $N \to \infty$: for example, there is a sharp threshold $p^* = 1/N$ below which the graph consists of many small isolated components and above which a single *giant component* containing a finite fraction of all nodes emerges almost surely. This *phase transition* in network connectivity was one of the first rigorous results connecting graph theory to the physics of phase transitions, and the Erdős–Rényi model served as the standard model for real-world networks for decades.

The modern era of network science began in the late 1990s with two landmark papers. In 1998, Watts and Strogatz showed that many real networks - ranging from the power grid of the western United States to the neural network of *C. elegans* to the collaboration graph of film actors — share a combination of properties that the Erdős–Rényi model cannot reproduce: high *clustering* (your friends tend to know each other) and short *average path length* (any two people are connected by a short chain of acquaintances) [28]. They termed this combination the *small-world property* and introduced a simple generative model that interpolates between a regular lattice and a random graph, reproducing both features simultaneously.

The following year, Barabási and Albert showed that many real networks display a *power-law degree distribution* - a small number of highly connected nodes (hubs) coexist with a large majority of poorly connected ones, and proposed that this *scale-free* structure arises from a growth process in which new nodes preferentially attach to already well-connected ones [29]. The discovery of scale-free networks had immediate implications for robustness: Albert, Jeong, and Barabási showed that scale-free networks are remarkably resilient to random failures but catastrophically vulnerable to targeted attacks on their hubs [5].

These discoveries triggered an explosion of research. In the two decades since, the field has moved beyond static structural analysis to study temporal networks, multilayer networks, adaptive networks, and, most relevant to this thesis, the dynamics of failure and recovery processes on complex topologies [19, 14, 1].

1.2.3 Basic Terminology and Notation

We now establish the notation used throughout this thesis. The connectivity structure of an undirected network is encoded in the *adjacency matrix* A, an $N \times N$ matrix whose entries

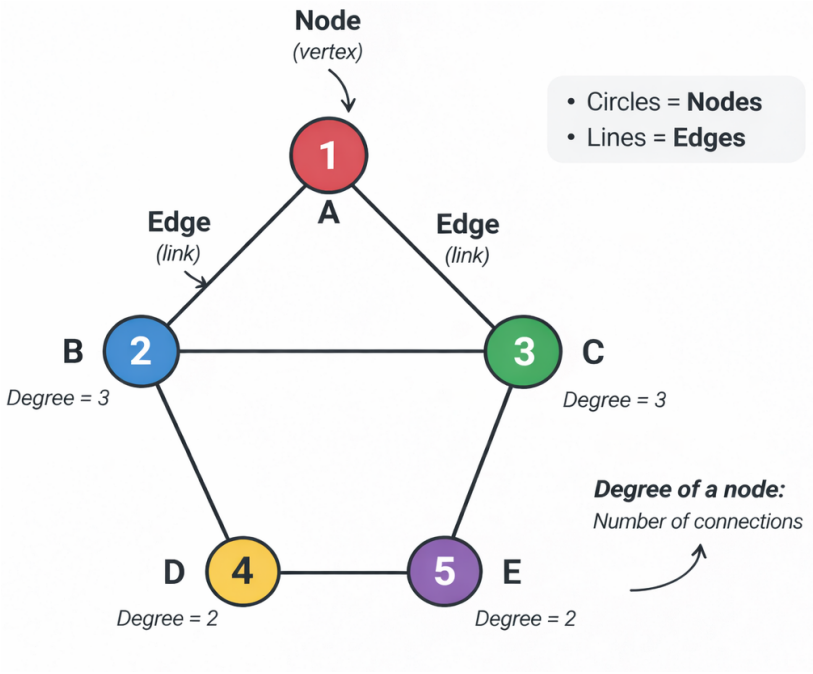


Figure 1.2: Schematic of a small undirected network. Filled circles represent nodes; lines represent edges. Labels beside nodes indicate degree.

are

$$A_{ij} = \begin{cases} 1, & \text{if there is an edge between nodes } i \text{ and } j, \\ 0, & \text{otherwise,} \end{cases} \tag{1.2}$$

with the convention $A_{ii} = 0$ (no self-loops). For an undirected network, A is symmetric: $A_{ij} = A_{ji}$. This symmetry means A has N real eigenvalues, which encode important spectral properties of the network. For weighted networks, A_{ij} is replaced by a non-negative weight w_{ij} representing the strength of the interaction. For directed networks, $A_{ij} = 1$ means there is an edge *from* i *to* j, and the matrix is in general asymmetric.

A schematic of a small undirected network is shown in Figure 1.2. The *degree* of a node i is the number of edges incident to it:

$$k_i = \sum_{j=1}^{N} A_{ij}. \tag{1.3}$$

The degree is perhaps the single most important local quantity characterizing a node's role in the network. For directed networks one distinguishes the *in-degree* $k_i^{\text{in}} = \sum_j A_{ji}$ from the *out-degree* $k_i^{\text{out}} = \sum_j A_{ij}$; conservation of edges implies $\sum_i k_i^{\text{in}} = \sum_i k_i^{\text{out}} = M$.

For an undirected network, each edge contributes 1 to the degree of each of its two endpoints, so the sum of all degrees equals twice the number of edges:

$$\sum_{i=1}^{N} k_i = 2M. \tag{1.4}$$

Equation (1.4) is sometimes called the *handshaking lemma* and holds for any simple undirected graph. The *average degree* is then

$$\langle k \rangle = \frac{1}{N} \sum_{i=1}^{N} k_i = \frac{2M}{N}. \tag{1.5}$$

The *degree distribution* $P(k)$ specifies the probability that a randomly chosen node has degree exactly k. It is the coarsest global summary of the network's heterogeneity, and as we shall see, it exerts a profound influence on almost every dynamical process occurring on the network.

1.2.4 Structural Properties of Networks

The following quantities provide a richer characterization of network structure beyond the degree distribution alone. Together they form a standard toolkit that is used throughout the thesis to describe and compare networks.

Degree Distribution

The degree distribution $P(k)$ is the probability mass function of node degrees. For the Erdős–Rényi random graph with connection probability p and large N, the degree of a typical node is binomially distributed. In the limit $N \to \infty$ with $\langle k \rangle = pN$ fixed, this converges to a Poisson distribution [26]:

$$P(k) = \frac{\langle k \rangle^k \, e^{-\langle k \rangle}}{k!}. \tag{1.6}$$

The Poisson distribution decays exponentially for $k \gg \langle k \rangle$, meaning that very high-degree nodes are essentially absent.

Many real networks, however, display a *heavy-tailed* degree distribution. The canonical case is the power law,

$$P(k) \sim k^{-\gamma}, \qquad k \geq k_{\min}, \tag{1.7}$$

with exponent γ typically in the range $2 < \gamma < 3$. Such networks are called *scale-free* because a power law is the only functional form invariant under rescaling $k \to ck$ [29, 1]. The heavy tail means that hubs — nodes with $k \gg \langle k \rangle$ — are not just possible but *expected* to exist in large networks, and they play a disproportionate role in all dynamical processes. For $\gamma \leq 3$, the variance of the degree distribution diverges with N, which has important consequences for processes such as epidemic spreading and cascading failures: in the infinite-network limit, there is no epidemic threshold, and a vanishingly small fraction of infected (or failing) nodes can infect (or bring down) the entire network [30].

Average Path Length and the Small-World Effect

A *walk* on a network is a sequence of nodes $v_0, v_1, \ldots, v_\ell$ such that each consecutive pair (v_{i-1}, v_i) is connected by an edge; a *path* is a walk in which no node is repeated. The *length* of a path is the number of edges it traverses. The *shortest path length* (or *geodesic distance*) d_{ij} between nodes i and j is defined as the minimum length over all paths connecting them. If no path exists, we set $d_{ij} = \infty$ by convention. For a connected network, all pairwise distances are finite, and the *average path length* is

$$L = \frac{1}{N(N-1)} \sum_{i \neq j} d_{ij}. \tag{1.8}$$

The average path length is a measure of how efficiently information or material can be transported across the network on average.

In a regular d-dimensional lattice, distances scale as $L \sim N^{1/d}$, which grows rapidly with system size. In Erdős–Rényi random graphs and in many real networks, however, L grows only as

$$L \sim \frac{\ln N}{\ln \langle k \rangle}, \tag{1.9}$$

which is remarkably slow [1]. This property — that even very large networks can be traversed in a small number of steps — is the celebrated *small-world effect*, first quantified rigorously by Watts and Strogatz [28]. The phrase "six degrees of separation" in social networks is a popular expression of this phenomenon.

A related but more extreme concept is the *ultra-small world* observed in scale-free networks with $2 < \gamma < 3$, where

$$L \sim \frac{\ln \ln N}{\ln(\gamma - 1)}, \tag{1.10}$$

meaning distances grow even more slowly than logarithmically [31]. This ultra-small-world property is a direct consequence of the presence of hubs, which act as highly efficient shortcuts.

The *diameter* of a network,

$$D = \max_{i,j} d_{ij}, \tag{1.11}$$

is the worst-case distance and provides an upper bound on how long any transfer of information or material can take. In practice, the diameter is typically only a small multiple of L for most networks.

Clustering Coefficient

Whereas the average path length measures global efficiency of traversal, the *clustering coefficient* measures local cohesion — the degree to which the neighbors of a node are also connected to each other. This is the network analog of the sociological observation that "the friend of my friend is also my friend."

The *local clustering coefficient* of node i (with $k_i \geq 2$) is defined as

$$C_i = \frac{2\, e_i}{k_i(k_i - 1)}, \tag{1.12}$$

where e_i is the number of edges that exist among the k_i neighbors of i, and $k_i(k_i-1)/2$ is the maximum possible number of such edges. Thus $C_i \in [0, 1]$, with $C_i = 1$ meaning that the neighborhood of i is a clique. The *global clustering coefficient* (also called the *transitivity*) of the network is the fraction of all connected triples that form closed triangles:

$$C_\Delta = \frac{3 \times \text{number of triangles}}{\text{number of connected triples}}. \tag{1.13}$$

A commonly used alternative is the *average clustering coefficient*,

$$\bar{C} = \frac{1}{N} \sum_{i=1}^{N} C_i. \tag{1.14}$$

In a random graph with large N, $C_\Delta \approx p = \langle k \rangle / N \to 0$, which is very small. Many real networks, by contrast, have clustering coefficients orders of magnitude larger — social networks typically have $\bar{C} \sim 0.1$–0.5 [28, 22]. High clustering combined with short path

lengths is the defining hallmark of the small-world regime.

Centrality Measures

Not all nodes are equally important. *Centrality measures* are scalar quantities assigned to nodes (or edges) that quantify their structural importance relative to some criterion — how many connections they have, how many shortest paths pass through them, how close they are to all others, or how important their neighbors are. Different measures capture different aspects of importance, and the choice of which to use depends on the dynamical process of interest [22, 32].

Degree Centrality. The most elementary measure is the degree k_i itself, or its normalized version,

$$C_D(i) = \frac{k_i}{N-1}. \tag{1.15}$$

Degree centrality captures the immediate influence of a node: highly connected nodes can directly reach — or be reached by — many others. In spreading processes, high-degree nodes are both the first to become infected and the most effective spreaders [30].

Betweenness Centrality. Betweenness centrality measures the extent to which a node lies on the shortest paths between other pairs of nodes. Let σ_{st} denote the total number of shortest paths from node s to node t, and let $\sigma_{st}(i)$ denote the number of those paths that pass through node i ($i \neq s$, $i \neq t$). Then the betweenness centrality of node i is

$$B_i = \sum_{\substack{s \neq t \\ s,t \neq i}} \frac{\sigma_{st}(i)}{\sigma_{st}}. \tag{1.16}$$

Nodes with high betweenness serve as bridges or bottlenecks in the network. Their removal disrupts the shortest paths between many pairs of nodes, making them critical for network connectivity [33]. Betweenness centrality is particularly relevant for studying cascading failures, because loads often distribute along shortest paths and high-betweenness nodes accumulate disproportionate load [12].

Closeness Centrality. A node is close (in the sense of closeness centrality) if it has small average geodesic distance to all other nodes. The closeness centrality of node i is

$$C_C(i) = \frac{N-1}{\sum_{j \neq i} d_{ij}}. \tag{1.17}$$

The factor $N-1$ normalizes $C_C(i)$ to lie in $(0, 1]$, with $C_C(i) = 1$ for a node connected to all others. Nodes with high closeness centrality are well-positioned to broadcast information or to monitor the network, since they are on average close to every other node [22].

Eigenvector Centrality. Degree centrality treats all neighbors equally, regardless of how important those neighbors themselves are. Eigenvector centrality addresses this by assigning to each node a score proportional to the sum of the scores of its neighbors:

$$x_i = \frac{1}{\lambda} \sum_{j=1}^{N} A_{ij}\, x_j, \tag{1.18}$$

where λ is a normalization constant. In matrix form, this is simply the eigenvalue equation

$$A\,\mathbf{x} = \lambda\,\mathbf{x}. \tag{1.19}$$

By the Perron–Frobenius theorem, if A is non-negative and irreducible (as it is for a connected network), there is a unique largest real eigenvalue λ_1, and its corresponding eigenvector has all positive components. The centrality scores are taken to be the components of this eigenvector [34]. Google's PageRank algorithm is a generalization of eigenvector centrality applied to the directed graph of the World Wide Web.

Network Density and Sparsity

The *density* of a network is the ratio of the actual number of edges to the maximum possible:

$$\rho = \frac{2M}{N(N-1)}, \tag{1.20}$$

where $N(N-1)/2$ is the number of edges in a complete graph K_N. A network with $\rho = 1$ is fully connected; most real-world networks have $\rho \ll 1$ and are said to be *sparse*. Sparsity is not just a practical observation — it has deep theoretical implications. Many analytical tools

in network science, such as mean-field approximations and generating function methods, are exact or highly accurate only in the sparse regime [22, 1].

Community Structure

Many real networks are not homogeneous but display *community structure*: a partition (or soft partition) of the node set into groups such that edges are much denser within groups than between them [35]. Communities correspond to functionally or topically coherent subunits: research groups in a collaboration network, protein complexes in a protein interaction network, or geographic clusters in a transportation network. Quantifying community structure is typically done via the *modularity* Q, defined as

$$Q = \frac{1}{2M} \sum_{i,j} \left(A_{ij} - \frac{k_i k_j}{2M} \right) \delta(c_i, c_j), \tag{1.21}$$

where c_i is the community to which node i is assigned and $\delta(c_i, c_j) = 1$ if i and j belong to the same community and 0 otherwise [36]. A modularity close to 1 indicates a strong community structure, while $Q \approx 0$ indicates that the network is no more modular than a random graph. Community structure is directly relevant to failure propagation: failures that originate within a tightly knit community may be temporarily contained by the sparse inter-community links, slowing the cascade [13].

1.2.5 Network Models

To develop theoretical understanding of empirically observed network properties, and to generate synthetic networks for computational experiments, a number of canonical generative models have been proposed. We discuss the three most widely used, each of which captures different aspects of real network topology. The degree distributions produced by these models are shown in Figure 1.3, illustrating the qualitative differences among them.

Erdős–Rényi Random Graph

In the $G(N, p)$ model introduced by Erdős and Rényi [26, 27], a network of N nodes is formed by connecting each of the $\binom{N}{2}$ possible pairs of nodes independently with probability p. The number of edges is a random variable with expectation

$$\langle M \rangle = p \, \frac{N(N-1)}{2}, \tag{1.22}$$

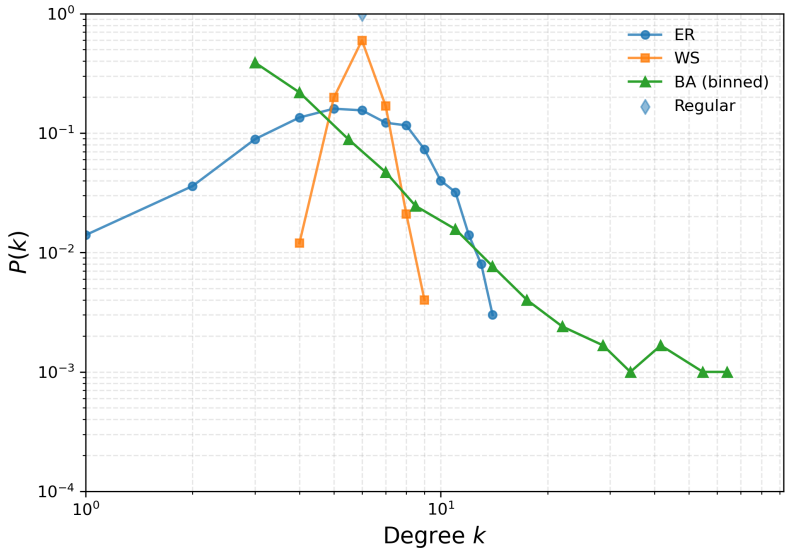


Figure 1.3: Degree distributions of four canonical network models on log-log axes ($N = 1000$, $\langle k \rangle = 6$). The Erdős–Rényi network shows a Poisson-like distribution, the Watts–Strogatz network a narrow distribution, and the Barabási–Albert network a broad power-law tail indicating the presence of hubs, and a single point for Regular/lattice network.

and the degree distribution converges to Eq. (1.6) for large N.

The ER model exhibits a sharp percolation phase transition. For $p < 1/N$ (equivalently $\langle k \rangle < 1$), the network consists of many small components, the largest of which has $O(\ln N)$ nodes. At $p = 1/N$, a giant component appears discontinuously and contains a finite fraction of all nodes for all $p > 1/N$ [27, 1]. This transition — the emergence of long-range connectivity — is a prototype for the percolation transitions studied in the context of network robustness.

The ER model is analytically tractable and provides important baseline results, but it fails to reproduce two of the most salient features of real networks: the heavy-tailed degree distribution and the high clustering coefficient.

Watts–Strogatz Small-World Model

Motivated by the coexistence of high clustering and short path lengths in real networks, Watts and Strogatz proposed a simple interpolation between an ordered lattice and a random graph [28]. Starting from a ring of N nodes in which each node is connected to its k nearest neighbors on each side (so initial degree is $2k$), each edge is independently rewired with probability p to a uniformly chosen random node, subject to no self-loops or duplicate edges.

When $p = 0$, the graph is a regular lattice with high clustering ($C \approx 3/4$ for large k) but long average path length ($L \approx N/2k$). When $p = 1$, the graph is essentially a random graph with low clustering but short path lengths. For intermediate values of p — say $10^{-3} \lesssim p \lesssim 10^{-1}$ — a small fraction of rewired edges dramatically reduces L while C remains close to its lattice value. This is the *small-world regime*: the rewired edges act as long-range shortcuts that collapse the diameter of the network without disrupting the local clustering structure [28].

The Watts–Strogatz model successfully reproduces the small-world property, but it still produces an approximately homogeneous (non-heavy-tailed) degree distribution. It therefore cannot account for the hubs observed in many real systems.

Barabási–Albert Scale-Free Model

To explain the origin of power-law degree distributions, Barabási and Albert proposed a dynamic model in which the network grows over time and new nodes preferentially attach to nodes that are already well-connected [29].

The construction proceeds as follows. Begin with a small seed network of m_0 nodes. At each time step, add one new node with $m \leq m_0$ edges. Each edge connects the new node to an existing node i with probability

$$\Pi(i) = \frac{k_i}{\sum_j k_j} = \frac{k_i}{2M_t}, \tag{1.23}$$

where M_t is the number of edges at time t and the denominator ensures normalization. This is *preferential attachment*: nodes with higher degree attract new connections at a higher rate, embodying a "rich-get-richer" dynamic.

After T time steps the network has $N = m_0 + T$ nodes and $M \approx mT$ edges. Using a mean-field argument [29] or the more rigorous master equation approach [37], one can show that the degree distribution converges to a power law

$$P(k) = \frac{2m^2}{k^3}, \qquad k \geq m, \tag{1.24}$$

which corresponds to $\gamma = 3$ in Eq. (1.7), independent of m.

The BA model captures the emergence of hubs and correctly predicts scale-free degree distributions in many real systems. However, it produces a clustering coefficient that decreases with N and is thus smaller than what is typically observed in real networks [38]. Various extensions have been proposed to address this, including models that incorporate fitness, aging, or additional triangle-closure mechanisms [39]. Nevertheless, the BA model remains the canonical reference for scale-free networks, and Eq. (1.23) and its consequences feature prominently in our analysis of failure dynamics later in this thesis.

Apollonian network Model

Apollonian networks are a class of deterministic, space-filling, and scale-free networks constructed through a recursive subdivision of planar graphs. The concept originates from the classical Apollonian gasket, a fractal generated by repeatedly filling the interstices between mutually tangent circles with further tangent circles. The construction begins with a triangle consisting of three mutually connected nodes. At each iteration, a new node is introduced inside an existing triangular face and is connected to all three vertices of that triangle. This process is repeated recursively for all newly formed triangular faces, resulting in a maximally planar graph where no additional edges can be added without violating planarity.

Apollonian networks exhibit several important structural characteristics. The degree distribution follows a power law,

$$P(k) \sim k^{-\gamma}, \quad \gamma \approx 2.58, \tag{1.25}$$

indicating the presence of highly connected hub nodes.Due to the triangular construction, these networks possess a high clustering coefficient, often close to unity for low-degree nodes. The average shortest path length grows logarithmically with system size, ensuring efficient connectivity (small world property). Older nodes acquire higher degrees over time, leading to strong degree correlations and a hierarchical structure.

1.2.6 Networks and Dynamical Processes

Network topology does not merely describe a static structure; it actively shapes — and is shaped by — the dynamics of processes that unfold on it. This coupling between structure and dynamics is what makes network science a genuinely interdisciplinary enterprise, drawing simultaneously on graph theory, statistical mechanics, and dynamical systems theory [23, 22, 32].

A wide variety of dynamical processes can occur on networks. *Spreading processes* — epidemics, rumors, cascading bank failures, computer viruses — propagate through contact along network edges [30]. In the susceptible-infected-susceptible (SIS) model on a network, the epidemic threshold λ_c is related to the spectral properties of the adjacency matrix:

$$\lambda_c = \frac{1}{\lambda_1}, \tag{1.26}$$

where λ_1 is the largest eigenvalue of A. For scale-free networks with $\gamma \leq 3$, λ_1 diverges with N, so $\lambda_c \to 0$: even an arbitrarily weak infection can spread through the network [30].

Synchronization of coupled oscillators on networks — relevant to power grids, neuronal circuits, and chemical reaction networks — depends on the spectral gap $\lambda_2 - \lambda_1$ (or equivalently the Fiedler value for Laplacian dynamics): a larger spectral gap promotes faster synchronization [40].

Random walks on networks provide a model for diffusive transport: a walker at node i moves to a neighbor j with probability A_{ij}/k_i. The stationary distribution of a random walk on an undirected network is proportional to node degree,

$$\pi_i = \frac{k_i}{2M}, \tag{1.27}$$

meaning that hubs are visited most frequently [41]. When multiple random walkers are present on the same network simultaneously, their collective occupation of nodes can fluctuate dramatically, producing rare events in which an unusually large number of walkers simultaneously visit the same node — these are the extreme events that form the central object of study in this thesis [8, 10].

Cascading failures represent a particularly consequential class of network dynamics [12, 42, 13]. In cascading failure models, each node or edge has a capacity for handling load. When a node fails, its load is redistributed to neighboring nodes. If a neighbor's load thereby exceeds its capacity, it too fails, and the process repeats. The outcome — whether the cascade arrests after a small number of failures or grows to consume a macroscopic fraction of the network — depends sensitively on the interplay between network topology, load distribution, and capacity margins [12, 17, 43]. Understanding this interplay, particularly when the initial trigger is an intrinsic fluctuation rather than an external attack, is a central theme of this thesis.

The connection between these dynamical processes and the structural properties introduced in the preceding sections is direct and explicit. Degree heterogeneity governs the stationary distribution of random walkers (Eq. 1.27), the epidemic threshold (Eq. 2.7), and the vulnerability of scale-free networks to hub-targeted attacks [5]. Clustering and community structure determine how quickly a cascade spreads from a local failure to the global network [13]. Betweenness centrality identifies the nodes through which the most load flows and hence those most likely to trigger a cascade when they fail [12, 10]. This tight coupling between structure and dynamics is why building a thorough understanding of network structure — as we have done in this chapter — is an essential prerequisite before studying the dynamical phenomena that are the main subject of this thesis.

1.2.7 Summary and Outlook

This chapter has laid the conceptual and mathematical groundwork for the rest of the thesis. We began with a discussion of the scientific and societal motivation for studying intrinsic failure mechanisms in complex networks, situating this work within the broader context of resilience science and statistical physics of extreme events. We then provided a self-contained introduction to complex network theory: the historical development of the field from Euler's graph theory through the modern discoveries of small-world and scale-free networks; the basic mathematical formalism of graphs, adjacency matrices, and degree sequences; the principal structural measures — degree distribution, clustering coefficient, path lengths, centrality, density, and community structure — and their physical interpretation; and the three canonical generative models — Erdős–Rényi, Watts–Strogatz, and Barabási–Albert — together with their analytical properties. Finally, we surveyed the major classes of dynamical processes on networks and established the connections between structural properties and dynamical behavior that will be exploited throughout the thesis.

The picture that emerges from this overview is that network structure is not a passive backdrop for dynamics but an active shaping force. Degree heterogeneity, clustering, and community organization each leave distinct signatures on spreading, synchronization, random walk, and failure dynamics. In the following chapters, we build directly on this foundation. Chapter 2 examines the dynamics of random walkers on networks in detail, deriving the statistical properties of node-occupation numbers and characterizing the conditions under which extreme events occur. Chapter 3 then uses these results as the starting point for a study of how locally triggered extreme events can drive global network failure, developing

a framework for understanding the onset, propagation, and aftermath of cascading breakdowns caused by intrinsic fluctuations. Chapter 4 then applies the repair mechanism on the network with flux, and looks for structural signatures in a network approaching failure.

Chapter 2

Dynamical Processes on Networks

2.1 Introduction

Many real-world systems are most naturally described as networks, in which nodes represent discrete interacting units and edges encode the relationships or interactions between them. While a large body of work has characterised the *structural* properties of such networks—degree distributions, clustering coefficients, path lengths, and centrality measures—the ultimate function of any networked system is determined by the *dynamical processes* that unfold on top of the structure [32, 22, 44]. Examples span an enormous range of scales and disciplines: the spreading of pathogens through human contact networks [45], synchronisation of generators in power grids [46], packet routing on the internet [47], cascading failures in interdependent infrastructure [48], and the diffusion of opinions in online social networks [49].

A unifying theme across all these settings is that the interplay between network topology and local node dynamics produces collective behaviour that is qualitatively different from—and far richer than—what arises in well-mixed or spatially regular systems. Heterogeneous degree distributions amplify fluctuations, shift phase-transition thresholds, and create hubs that dominate transport, spreading, and failure dynamics [29, 50]. Understanding these effects is therefore central to the study of robustness, resilience, and controllability of complex systems.

This chapter develops the theoretical framework used throughout this thesis to study dynam-

ical processes on networks. Section 2.2 introduces the general mathematical representation of network dynamics. Sections 2.6–2.7 survey the principal classes of dynamics that arise in practice. Section 2.8 develops the random-walk flux model that underpins the extreme-event analysis in subsequent chapters.

2.2 Mathematical Representation of Network Dynamics

Let $G = (V, E)$ be an undirected, unweighted graph with $|V| = N$ nodes and adjacency matrix $\mathbf{A}$, so that $A_{ij} = 1$ if $(i, j) \in E$ and $A_{ij} = 0$ otherwise. Denote the degree of node i by $k_i = \sum_j A_{ij}$. Let $x_i(t) \in \mathbb{R}$ be the state variable of node i at time t. A broad class of continuous-time network dynamics can be written in the generic form

$$\frac{dx_i}{dt} = F(x_i) + \sum_{j=1}^{N} A_{ij}\, G(x_i, x_j), \tag{2.1}$$

where $F : \mathbb{R} \to \mathbb{R}$ governs the intrinsic (self-)dynamics of each node and $G : \mathbb{R}^2 \to \mathbb{R}$ encodes the pairwise coupling between adjacent nodes [51]. Equation (2.1) captures diffusion ($F = 0$, $G = x_j - x_i$), synchronisation (Kuramoto coupling), epidemic spreading (SIS/SIR mean-field), and many other processes as special cases.

2.2.1 Dynamics *on* vs. Dynamics *of* Networks

It is important to distinguish two regimes [52]:

- **Dynamics on networks.** The adjacency matrix $\mathbf{A}$ is fixed and only the state variables $\{x_i(t)\}$ evolve. This framework isolates the influence of topology on dynamical behaviour and is the setting adopted throughout this chapter.

- **Dynamics of networks.** Both $\{x_i(t)\}$ and $\mathbf{A}(t)$ evolve simultaneously. Examples include adaptive rewiring in social networks, growing citation graphs, and co-evolutionary disease-behaviour systems. Such systems can exhibit feedback between state and structure, generating phenomena such as echo-chamber formation and explosive percolation [53].

Many real systems belong to neither extreme but lie in an intermediate regime where

structural and dynamical timescales are comparable. The theoretical treatment of such co-evolutionary systems remains an active area of research.

2.2.2 Graph Laplacian and Spectral Properties

A central operator in network dynamics is the *graph Laplacian*

$$L_{ij} = k_i\,\delta_{ij} - A_{ij}, \tag{2.2}$$

where δ_{ij} is the Kronecker delta and $\mathbf{D} = \mathrm{diag}(k_1, \ldots, k_N)$ is the degree matrix, so that $\mathbf{L} = \mathbf{D} - \mathbf{A}$. The Laplacian is positive semi-definite; its eigenvalues $0 = \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_N$ encode fundamental properties of the graph. The smallest non-zero eigenvalue λ_2 (the *algebraic connectivity* or *Fiedler value*) measures how well-connected the graph is, while the ratio $R = \lambda_N/\lambda_2$ governs synchronisability via the master stability function (see Section 2.5) [40]. The Laplacian also governs diffusion and random-walk dynamics, as discussed in Section 2.7.

2.3 Percolation and Network Resilience

Percolation theory is the simplest yet most fundamental dynamical process on a network. In *site percolation*, nodes are independently removed with probability $1-p$; in *bond percolation*, edges are removed. The central question is: for what value of p does a macroscopic *giant connected component* (GCC) survive? The answer defines the network's resilience to random failures or targeted attacks [54].

2.3.1 Erdős–Rényi Networks

For an Erdős–Rényi (ER) graph $\mathcal{G}(N, \langle k\rangle/N)$ with mean degree $\langle k\rangle$, the percolation threshold for site removal is [55]

$$p_c = \frac{1}{\langle k\rangle}. \tag{2.3}$$

Below p_c the GCC collapses to $\mathcal{O}(\log N)$ nodes; above it, a GCC of size $\mathcal{O}(N)$ exists. The transition is second-order in the infinite-size limit.

2.3.2 Scale-Free Networks

The analysis changes dramatically for scale-free networks with degree distribution $P(k) \sim k^{-\gamma}$. Using generating-function methods [56], the condition for the existence of a GCC is

$$\kappa \equiv \frac{\langle k^2 \rangle}{\langle k \rangle} > 2. \tag{2.4}$$

Albert, Jeong, and Barabási showed that for $\gamma \leq 3$, the second moment $\langle k^2 \rangle$ diverges as $N \to \infty$, so $p_c \to 0$ [5]. Scale-free networks are therefore *exceptionally resilient to random failures*: since the vast majority of nodes have low degree, random removal rarely strikes a hub. However, the same networks are *extremely vulnerable to targeted attacks*: sequential removal of the highest-degree nodes rapidly destroys the GCC, with a vanishing attack threshold in the infinite-size limit [6]. This robustness-yet-fragility duality has profound implications for the design and protection of technological and biological networks.

2.3.3 Generating-Function Formalism

A powerful analytical tool for percolation on arbitrary degree sequences is the generating-function (GF) framework of Newman, Strogatz, and Watts [56]. Define the probability-generating function of the degree distribution $G_0(x) = \sum_k P(k) x^k$ and the excess-degree generating function $G_1(x) = G_0'(x)/\langle k \rangle$. The GCC size S satisfies the self-consistency equation

$$S = 1 - G_0(u), \qquad u = G_1(u), \tag{2.5}$$

where u is the probability that a randomly chosen edge does *not* lead to the GCC. This framework has been extended to correlated networks [57], degree-heterogeneous site percolation [54], and the SIR epidemic mapping discussed in Section 2.4.

2.4 Epidemic Spreading

The propagation of infectious diseases on networks is one of the most intensively studied dynamical processes in statistical physics and mathematical epidemiology [58, 59]. Classical well-mixed (mass-action) models are the special case in which the contact network is a complete graph; on sparse heterogeneous networks the behaviour is qualitatively different.

2.4.1 Compartmental Models

SI Model. In the Susceptible–Infected (SI) model each node is in one of two states. Infection is transmitted across an edge at rate β; there is no recovery. The SI model describes the early exponential growth phase of an epidemic and yields the logistic infection curve for well-mixed populations. On networks, the epidemic front propagates at a speed determined by the shortest-path structure.

SIS Model. In the Susceptible–Infected–Susceptible (SIS) model, infected nodes recover to the susceptible state at rate μ, enabling reinfection. Define the effective spreading rate $\lambda = \beta/\mu$. The mean-field equation for the infection probability $\rho_i(t)$ of node i is [60]

$$\frac{d\rho_i}{dt} = -\mu\,\rho_i + \beta\,(1-\rho_i)\sum_{j=1}^{N} A_{ij}\,\rho_j. \tag{2.6}$$

Linearising around the disease-free fixed point $\rho_i = 0$ shows that the epidemic threshold is [61]

$$\lambda_c = \frac{1}{\Lambda_m}, \tag{2.7}$$

where Λ_m is the spectral radius (largest eigenvalue) of $\mathbf{A}$. For a random network with degree distribution $P(k)$, $\Lambda_m \approx \sqrt{\langle k^2\rangle/\langle k\rangle}$ (heterogeneous mean-field approximation), giving

$$\lambda_c \approx \frac{\langle k\rangle}{\langle k^2\rangle}. \tag{2.8}$$

For scale-free networks with $\gamma \leq 3$, the divergence of $\langle k^2\rangle$ drives $\lambda_c \to 0$ in the thermodynamic limit [45]. This landmark result—that *no* non-zero epidemic threshold exists in heterogeneous scale-free networks—has reshaped public-health strategies: random vaccination is ineffective, while targeted immunisation of hubs can restore a finite threshold [31].

SIR Model. In the Susceptible–Infected–Recovered (SIR) model, recovery confers permanent immunity. The final epidemic size $R(\infty)$ is related to bond percolation on the contact network, with transmissibility $T = 1 - e^{-\beta/\mu}$ playing the role of bond occupation probability [62, 63]. This mapping allows the GF formalism to provide exact results for the epidemic threshold and final size on configuration-model networks. The comparison between the SI, SIS and SIR models are shown in the figure 2.1.

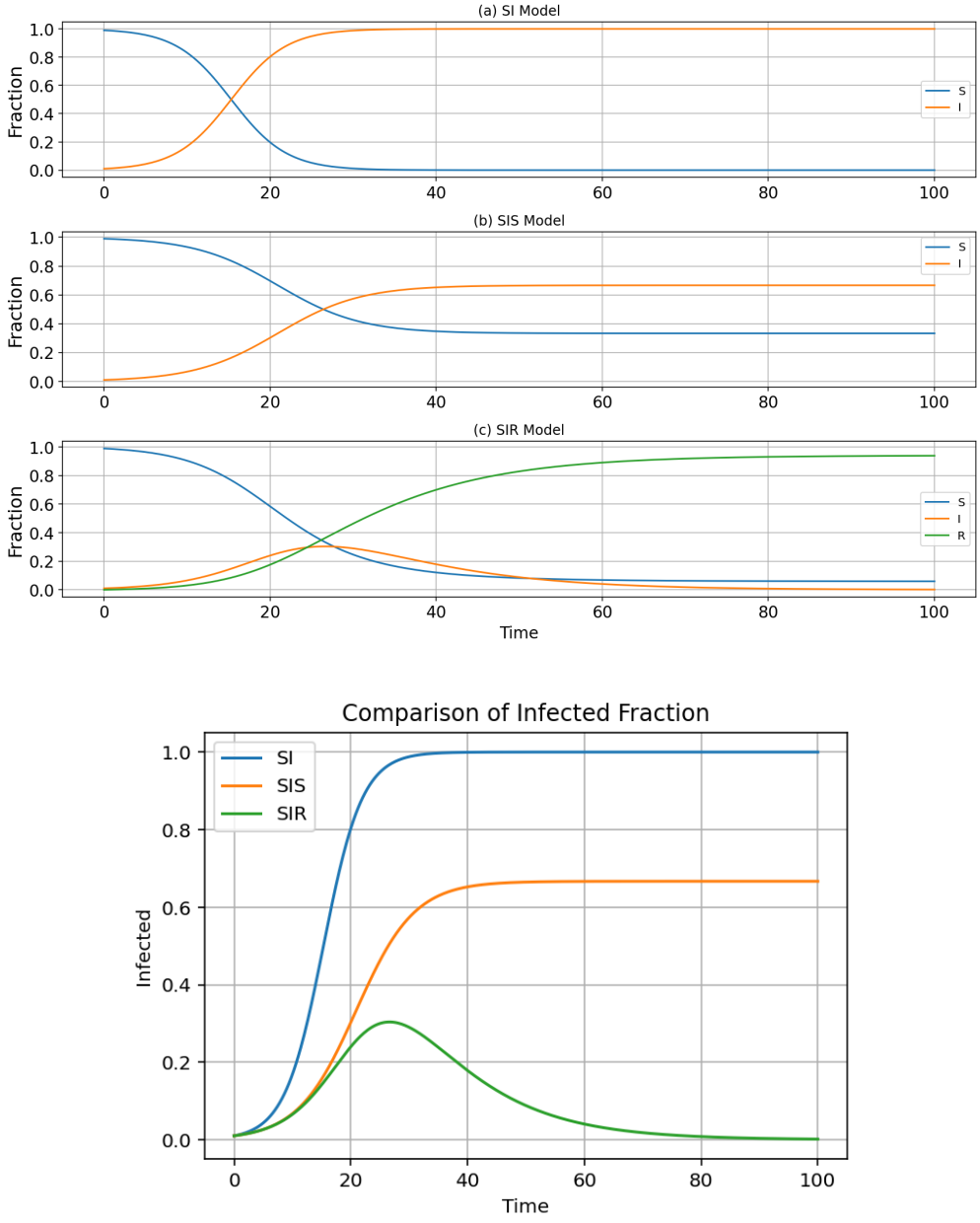


Figure 2.1: Epidemic models (top) Shows the three models: SI, SIS and SIR. (bottom) Comparison between fraction of infected individuals across the models.

2.4.2 Mean-Field Theories

Heterogeneous Mean-Field (HMF). Pastor-Satorras and Vespignani introduced the degree-based or *heterogeneous* mean-field (HMF) approximation [30, 45]: all nodes of degree k are assumed statistically equivalent, and one writes equations for $\rho_k(t)$, the fraction of degree-k nodes that are infected. For the SIS model,

$$\frac{d\rho_k}{dt} = -\mu\,\rho_k + \beta\,k\,(1-\rho_k)\,\Theta(t), \qquad \Theta(t) = \frac{1}{\langle k\rangle}\sum_k k\,P(k)\,\rho_k(t), \tag{2.9}$$

where $\Theta(t)$ is the probability that a randomly chosen neighbour is infected. HMF correctly predicts the vanishing threshold in scale-free networks and captures the degree-stratified dynamics.

Quenched Mean-Field (QMF). The *quenched* mean-field theory retains information about individual nodes via equation (2.6), yielding the threshold (2.7) [61]. QMF is more accurate than HMF on real (correlated) networks but involves solving an N-dimensional system.

Dynamic Message-Passing (DMP). The dynamic message-passing algorithm [64] provides a non-linear pair-level closure that is exact on trees and highly accurate on locally tree-like sparse networks. DMP gives the best analytical predictions for SIR epidemic size and timing on single network realisations, outperforming both HMF and QMF in the presence of degree correlations.

2.5 Synchronisation

Synchronisation—the spontaneous emergence of coherent collective oscillation among coupled dynamical units—occurs in power grids, cardiac pacemakers, neuronal assemblies, and chemical oscillator arrays [65, 51]. The paradigmatic model is the Kuramoto model.

2.5.1 Kuramoto Model

Consider N phase oscillators with natural frequencies $\{\omega_i\}$ drawn from a distribution $g(\omega)$ (typically unimodal and symmetric). The phase $\theta_i(t)$ evolves as [66, 67]

$$\dot{\theta}_i = \omega_i + K \sum_{j=1}^{N} A_{ij} \sin(\theta_j - \theta_i), \tag{2.10}$$

where $K \geq 0$ is the global coupling strength. Synchrony is quantified by the complex order parameter

$$r(t)\, e^{\mathrm{i}\psi(t)} = \frac{1}{N} \sum_{j=1}^{N} e^{\mathrm{i}\theta_j(t)}, \tag{2.11}$$

with $r \in [0, 1]$: $r = 0$ indicates incoherence and $r = 1$ full synchronisation.

On a complete graph, the model undergoes a continuous (second-order) phase transition at $K_c = 2/(\pi g(0))$ [66]. For $K < K_c$ the system is incoherent; for $K > K_c$ a macroscopically synchronised cluster forms and $r \sim \sqrt{K - K_c}$.

2.5.2 Synchronisation on Complex Networks

On heterogeneous networks the behaviour depends on γ. For $\gamma > 3$, the transition is mean-field-like with $K_c \sim 1/\Lambda_m$. For $2 < \gamma \leq 3$, the natural frequency heterogeneity induced by degree correlations (when $\omega_i \propto k_i$) can produce a *explosive* (first-order) synchronisation transition via a hysteresis loop [68]. Networks with community structure exhibit a two-stage synchronisation process: intra-community coherence precedes inter-community synchronisation [69].

2.5.3 Master Stability Function

The *master stability function* (MSF) framework of Pecora and Carroll [40] provides a topology-agnostic criterion for synchronisation stability. For a network of identical oscillators described by $\dot{\mathbf{x}}_i = \mathbf{F}(\mathbf{x}_i) + K \sum_j A_{ij} \mathbf{H}(\mathbf{x}_j)$, the stability of the synchronised manifold is determined by the Laplacian eigenvalues $\{\lambda_i\}$. The maximum Lyapunov exponent $\sigma_{\max}$ is a function of $K\lambda_i$; stability requires $\sigma_{\max}(K\lambda_i) < 0$ for all $i \geq 2$. The *synchronisability ratio*

$$R = \frac{\lambda_N}{\lambda_2} \tag{2.12}$$

measures how wide the range of stable coupling values is: a smaller R implies better synchronisability [70]. Homogeneous degree distributions and certain modular topologies minimise R, providing design principles for synchronisable networks.

2.6 Social Dynamics and Opinion Formation

Networks are the natural substrate for the propagation of ideas, opinions, norms, and behaviours. The statistical physics of social dynamics aims to derive macroscopic collective phenomena—consensus, polarisation, cultural diversity—from microscopic interaction rules [71].

2.6.1 Voter Model

In the voter model each node holds one of two opinions $\{0, 1\}$. At each discrete time step, a randomly selected node i copies the opinion of a randomly chosen neighbour. On a well-mixed population consensus is absorbed in $\mathcal{O}(N)$ steps; on a one-dimensional lattice the consensus time scales as N^2; on a complete graph it scales as $N \log N$ [72]. On heterogeneous complex networks, hubs act as opinion leaders: the consensus time becomes dominated by the inverse of the lowest non-zero Laplacian eigenvalue, scaling as $N\langle k\rangle/\langle k^2\rangle$ for uncorrelated networks [73]. The voter model is equivalent to coalescing random walks and is exactly solvable via the duality relation between the forward dynamics and the ancestral coalescence process [74].

2.6.2 Threshold Models

Granovetter's threshold model [75] and its network generalisation by Watts [49] capture the idea that individuals adopt a new behaviour only after a sufficient fraction of their social contacts have done so. Each node i has threshold $\phi_i \in [0, 1]$; a susceptible node activates when the fraction of active neighbours exceeds ϕ_i. Starting from a small seed, a *global cascade* propagates if and only if a percolating cluster of *vulnerable* nodes (those with $\phi_i < 1/k_i$) exists [49]. The cascade condition, expressed in terms of the degree distribution and threshold distribution, predicts a non-monotone dependence on network connectivity: both too-sparse and too-dense networks resist global cascades, while intermediate connectivity maximises susceptibility. Threshold models have been applied to financial contagion [76], political mobilisation, and viral marketing.

2.6.3 Evolutionary Game Theory on Networks

Evolutionary game theory investigates how strategic interactions among agents shape the population-level distribution of behaviours [77]. In the *Prisoner's Dilemma* (PD), cooperators (C) and defectors (D) interact; mutual cooperation yields reward R, mutual defection yields punishment P, and a defector paired with a cooperator earns the temptation payoff $T > R > P > S$ (sucker's payoff). In a well-mixed population, defection is the evolutionarily stable strategy. On networks, spatial reciprocity enables cooperation to persist: cooperators form clusters that resist invasion by defectors [78, 79]. On scale-free networks, hubs that adopt cooperation sustain cooperative behaviour across their large neighbourhoods, strongly promoting network reciprocity [79]. The payoff of a hub-cooperator scales with its degree, providing a strong selective advantage that is absent in homogeneous networks. Network reciprocity is now recognised as one of the five key mechanisms for the evolution of cooperation alongside kin selection, direct reciprocity, indirect reciprocity, and group selection [77].

2.7 Diffusion and Random Walk Processes

Diffusion is the most fundamental transport process on networks and the theoretical basis for the random-walk flux model developed in the next section. Let $p_i(t)$ denote the probability that a random walker occupies node i at time t. The continuous-time master equation is [41]

$$\frac{dp_i}{dt} = \sum_{j=1}^{N} L_{ij}\, p_j, \tag{2.13}$$

where $\mathbf{L}$ is the graph Laplacian (2.2). The general solution is

$$\mathbf{p}(t) = e^{-\mathbf{L}t}\,\mathbf{p}(0) = \sum_{i=1}^{N} c_i\,\mathbf{v}_i\, e^{-\lambda_i t}, \tag{2.14}$$

where $\{\lambda_i, \mathbf{v}_i\}$ are eigenpairs of $\mathbf{L}$ and c_i are set by initial conditions. Because $\lambda_1 = 0$ with eigenvector $\mathbf{1}$, the system relaxes to the stationary distribution at a rate set by λ_2 (the spectral gap). For an undirected connected graph the stationary distribution is [80]

$$p_i^{*} = \frac{k_i}{2|E|} = \frac{k_i}{\sum_j k_j}, \tag{2.15}$$

so that high-degree nodes are visited proportionally more often. The mixing time—the time to reach stationarity from an arbitrary initial distribution—scales as $\mathcal{O}(1/\lambda_2)$ [80]. On scale-free networks, the small spectral gap leads to slow mixing and a wide separation between hub and leaf visitation frequencies.

2.7.1 Cascading Failures

Many infrastructure networks exhibit cascading failure dynamics in which the overload of one node triggers redistributions that exceed the capacity of other nodes, propagating the failure throughout the system [12, 42]. In the load-capacity model, each node i carries a steady-state load L_i (e.g. betweenness centrality) and a capacity

$$C_i = (1 + \alpha)\, L_i, \tag{2.16}$$

where $\alpha \geq 0$ is the tolerance parameter. The failure of a node redistributes its load to the remaining network; if any node j thereby satisfies $L_j > C_j$, it too fails, initiating a cascade [12]. On scale-free networks, targeted removal of high-betweenness hubs triggers system-wide cascades even for moderate α [42]. Increasing α provides resilience but at a cost proportional to network size, posing a design trade-off between robustness and efficiency.

2.8 Random Walk Flux Dynamics and Extreme Events

2.8.1 Introduction

Transport processes in real-world networked systems—packet routing on the internet, vehicular flow in urban road networks, power transmission in electrical grids—are inherently stochastic. Local fluctuations in the number of entities passing through a node can occasionally exceed the node's service capacity, producing *extreme events*: brief but severe overload episodes that can trigger congestion, equipment failure, or cascading disruptions [81, 82]. Characterising the statistical properties of such fluctuations is therefore essential for assessing network robustness. The random-walk model provides a tractable yet realistic framework for this purpose.

2.8.2 Model Definition

Consider a connected undirected network of N nodes with adjacency matrix $\mathbf{A}$ and W non-interacting random walkers. At each discrete time step, every walker at node i independently hops to one of its k_i neighbours with uniform probability:

$$P_{ij} = \frac{A_{ij}}{k_i}. \tag{2.17}$$

The time evolution of the single-walker probability distribution obeys the master equation

$$P_i(t+1) = \sum_{j=1}^{N} P_j(t)\,\frac{A_{ji}}{k_j}. \tag{2.18}$$

In the stationary regime the distribution is given by equation (2.15), confirming that high-degree nodes attract a proportionally larger share of walkers.

2.8.3 Flux Distribution

Define the *flux* f_i at node i as the number of walkers visiting i during a time window of length T. In the stationary state, each walker visits i at each step with probability $P_i^* = k_i / \sum_j k_j$. For W independent walkers and a single time step ($T = 1$), the flux follows a binomial distribution:

$$P(f_i = w) = \binom{W}{w} (P_i^*)^w \,(1 - P_i^*)^{W-w}, \tag{2.19}$$

with mean and variance

$$\langle f_i \rangle = W\,P_i^* = \frac{W k_i}{\sum_j k_j}, \tag{2.20}$$

$$\sigma_i^2 = W\,P_i^*(1 - P_i^*) \approx W\,P_i^* \quad \text{for sparse networks.} \tag{2.21}$$

Both the mean and the standard deviation of the flux are therefore proportional to $\sqrt{k_i}$ (in relative terms), so high-degree nodes carry larger absolute fluctuations.

2.8.4 Definition and Probability of Extreme Events

An *extreme event* at node i is defined as a realisation in which the flux exceeds a degree-dependent threshold q_i:

$$f_i > q_i, \qquad q_i = \langle f_i \rangle + m\,\sigma_i, \tag{2.22}$$

where $m > 0$ is a control parameter that sets how many standard deviations above the mean the threshold lies. Large m corresponds to rarer, more extreme events. The extreme-event probability at node i is

$$\mathcal{F}_i(m) = \sum_{w=\lceil q_i \rceil}^{W} \binom{W}{w} (P_i^*)^w \, (1 - P_i^*)^{W-w}, \tag{2.23}$$

which depends on the network topology through P_i^* and therefore through k_i.

2.8.5 Degree Dependence of Extreme-Event Statistics

Since $\langle f_i \rangle \propto k_i$ and $\sigma_i \propto \sqrt{k_i}$, the threshold q_i grows with k_i but the coefficient of variation $\sigma_i / \langle f_i \rangle \propto k_i^{-1/2}$ *decreases*. This means that in relative terms, low-degree nodes experience larger fluctuations around their mean. However, the absolute excess $(f_i - \langle f_i \rangle)$ is largest at hubs, so their overload events are the most severe in magnitude. The complex interplay between relative and absolute fluctuations determines the vulnerability profile of the network and is analysed in detail in the next section using Extreme Value Theory.

For heavy-tailed degree distributions ($\gamma \leq 3$), the diverging moments amplify fluctuations further, leading to *Fréchet*-type extreme value statistics at hubs rather than the Gumbel tail expected for homogeneous networks [82].

2.8.6 Implications for Network Robustness

The results above have several practical consequences:

1. **Congestion hotspots.** Hubs are the most likely locations for absolute overload events. Capacity-planning models must account for the degree-scaling of flux moments, not merely the mean load [81].

2. **Cascade initiation.** An extreme event at a hub can redistribute load to its k_i neighbours simultaneously, potentially triggering a cascade if their capacities are insufficient [12].

3. **Mitigation strategies.** Increasing hub capacity (targeted hardening), introducing flow-control mechanisms that redistribute walkers before overload, or rewiring the network to reduce Λ_m are all effective, and their relative costs can be evaluated within the random-walk framework.

2.9 Extreme Value Theory

2.9.1 Introduction and Motivation

Extreme events—rare yet high-impact occurrences—govern risk in a wide range of disciplines: financial market crashes [83], record-breaking floods and heat waves [84], material fatigue and structural failure [20], and traffic congestion in communication networks [82]. Classical statistics, which concerns itself primarily with averages and typical fluctuations, is ill-suited to describe such events: the tail of a distribution controls the probability of extremes, and tails are sensitive to the parent distribution in ways that the central limit theorem does not capture.

Extreme Value Theory (EVT) is the branch of probability theory devoted to the stochastic behaviour of maxima and minima of random samples. It provides a rigorous, universal characterisation of tail behaviour analogous to the central limit theorem for sums: just as sums of i.i.d. random variables converge to a Gaussian regardless of the parent distribution, suitably normalised maxima converge to one of three universal extreme-value distributions [85, 86, 87]. This universality makes EVT a powerful tool for extrapolating beyond observed data ranges.

In the context of dynamical processes on complex networks, extreme events arise from intrinsic stochastic fluctuations in node flux, load, and inter-arrival times. EVT provides the natural framework to quantify their probability, return periods, and dependence on network topology—forming the theoretical backbone of the analysis in subsequent chapters.

2.9.2 Classical Extreme Value Problem

Let $X_1, X_2, \ldots, X_n$ be independent and identically distributed (i.i.d.) random variables with common cumulative distribution function (CDF) $F(x)$. Define the sample maximum

$$M_n = \max\{X_1, X_2, \ldots, X_n\}. \tag{2.24}$$

The exact CDF of M_n is $P(M_n \leq x) = [F(x)]^n$, which concentrates near the upper endpoint of F as $n \to \infty$ and is therefore degenerate without rescaling. The central problem of EVT is to identify sequences of constants $a_n > 0$ and $b_n \in \mathbb{R}$ such that the normalised maximum

$$\frac{M_n - b_n}{a_n} \xrightarrow{d} G(x) \tag{2.25}$$

converges in distribution to a non-degenerate limit G.

2.9.3 Fisher–Tippett–Gnedenko Theorem

[Fisher–Tippett–Gnedenko [85, 86]] If there exist normalising constants $a_n > 0$ and $b_n \in \mathbb{R}$ such that (2.25) holds with a non-degenerate limit G, then G must belong to one of three families: the *Gumbel*, *Fréchet*, or *Weibull* distributions.

This result—the extreme-value analogue of the central limit theorem—underpins all of classical EVT. The three families are characterised by the tail behaviour of the parent distribution F.

Gumbel Distribution (Type I)

$$G(x) = \exp\bigl(-e^{-x}\bigr), \qquad x \in \mathbb{R}. \tag{2.26}$$

The Gumbel distribution arises from parent distributions with exponentially bounded tails, such as the Gaussian, exponential, and log-normal families. The normalising constants are $b_n = F^{-1}(1 - 1/n)$ and $a_n = 1/(nf(b_n))$, where f is the density of F. This is the *lightest* tail of the three families.

Fréchet Distribution (Type II)

$$G(x) = \begin{cases} 0, & x \le 0, \\ \exp\bigl(-x^{-\alpha}\bigr), & x > 0, \end{cases} \qquad \alpha > 0. \tag{2.27}$$

The Fréchet distribution arises from heavy-tailed, power-law parent distributions: $F(x) \sim 1 - cx^{-\alpha}$ as $x \to \infty$ (regularly varying tails with index α). The shape parameter α equals the tail index of F: smaller α means a heavier tail and more extreme events. Power-law degree distributions in scale-free networks ($P(k) \sim k^{-\gamma}$, $\alpha = \gamma - 1$) fall in this domain of attraction, so flux maxima on scale-free networks follow Fréchet statistics [82].

Weibull Distribution (Type III)

$$G(x) = \begin{cases} \exp\bigl(-(-x)^{\alpha}\bigr), & x \le 0, \\ 1, & x > 0, \end{cases} \qquad \alpha > 0. \tag{2.28}$$

The Weibull (or reversed Weibull) distribution arises when F has a finite upper endpoint $x^* < \infty$ with $F(x) \sim 1 - c(x^* - x)^{\alpha}$ near x^*. This applies to bounded random variables such

as the uniform distribution on $[0, 1]$.

2.9.4 Generalised Extreme Value Distribution

The three types can be unified into the *Generalised Extreme Value* (GEV) distribution [88, 87]:

$$G(x;\, \mu, \sigma, \xi) = \exp\left[-\left(1 + \xi\, \frac{x-\mu}{\sigma} \right)_+^{-1/\xi} \right], \tag{2.29}$$

where $(u)_+ = \max(u, 0)$, $\mu \in \mathbb{R}$ is the location parameter, $\sigma > 0$ is the scale parameter, and $\xi \in \mathbb{R}$ is the *shape* (or tail-index) parameter. The three classical families are recovered as:

- $\xi = 0$ (limit $\xi \to 0$): Gumbel — exponential tail;
- $\xi > 0$: Fréchet — heavy (power-law) tail, $\xi = 1/\alpha$;
- $\xi < 0$: Weibull — finite upper bound.

The GEV provides a unified framework for parameter estimation and model selection: fitting a single three-parameter family and inspecting $\hat{\xi}$ reveals the tail class without prior specification.

Block Maxima Method

The principal inferential method based on (2.29) is the *block maxima* approach [87]: divide a long time series into blocks of length n, extract the maximum from each block, and fit the resulting sample $\{M_n^{(1)}, M_n^{(2)}, \ldots\}$ to the GEV by maximum likelihood or L-moments. The asymptotic justification requires n to be large enough that the GEV approximation is accurate, while the number of blocks must be sufficient for stable estimation. Annual maxima in hydrology and climate science are the canonical application [84].

Peaks Over Threshold Method

The block maxima method discards all non-maximal values and may be wasteful. The *Peaks Over Threshold* (POT) method exploits all exceedances above a high threshold u [89, 90, 87]. We have used this in our thesis work, which wil be presented in the next chapter.

Generalised Pareto Distribution

Let $Y = X - u$ be the excess above u, conditional on $X > u$. The Pickands–Balkema–de Haan theorem states that, for sufficiently high u, the distribution of Y is approximated by the *Generalised Pareto Distribution* (GPD) [91, 89]:

$$H(y;\, \xi, \beta) = 1 - \left(1 + \xi\, \frac{y}{\beta}\right)_{+}^{-1/\xi}, \qquad y \geq 0, \tag{2.30}$$

with scale $\beta > 0$ and shape $\xi \in \mathbb{R}$. The shape parameter ξ in (2.30) is the same as in the GEV (2.29): $\xi = 0$ gives an exponential tail, $\xi > 0$ a Pareto (power-law) tail, and $\xi < 0$ a bounded tail.

Threshold Selection

A critical practical issue is the choice of u. Too low a threshold introduces bias (the GPD approximation is inaccurate); too high reduces the sample of exceedances and inflates variance. Standard diagnostic tools include:

- *Mean residual life plot*: $\mathbb{E}[X - u \mid X > u]$ should be approximately linear in u above the true threshold [87];
- *Parameter stability plot*: estimates of ξ and β (suitably reparametrised) should stabilise above the threshold.

In network applications, the threshold is often set analytically as $q_i = \langle f_i \rangle + m\sigma_i$ (equation (2.22)), combining network-structural information with statistical considerations [82].

2.9.5 Return Levels and Recurrence Times

Return Level

The *T-observation return level* x_T is defined implicitly by

$$P(X > x_T) = \frac{1}{T}, \tag{2.31}$$

meaning that x_T is exceeded on average once every T observations. Equivalently, $x_T = F^{-1}(1 - 1/T)$. For the GEV,

$$x_T = \mu - \frac{\sigma}{\xi}\left[1 - (-\log(1 - T^{-1}))^{-\xi}\right]. \tag{2.32}$$

Return levels are the primary output of operational EVT analyses in hydrology, wind engineering, and insurance [84, 83].

Recurrence Time Statistics

The recurrence time τ between successive extreme events—defined as the inter-arrival time between exceedances of q_i—carries dynamical information beyond the marginal distribution. For i.i.d. processes, τ is geometrically (in discrete time) or exponentially (in continuous time) distributed with mean $\langle\tau\rangle = 1/\mathcal{F}_i(m)$:

$$P(\tau > t) = e^{-t/\langle\tau\rangle}. \tag{2.33}$$

Deviations from exponential recurrence indicate temporal correlations and memory in the underlying process. In particular, *power-law* recurrence distributions,

$$P(\tau > t) \sim t^{-\nu}, \tag{2.34}$$

signal long-range correlations and have been observed in climate extremes [92], financial volatility, and network transport dynamics [82]. Characterising the recurrence statistics of extreme flux events at individual nodes—and how they depend on node degree and network topology—is a principal goal of this thesis.

2.9.6 Extreme Events on Complex Networks

Topological Influence on Extreme Value Statistics

The network topology shapes extreme-event statistics in three principal ways.

Degree heterogeneity. From equations (2.20)–(2.21), the flux moments at node i scale with k_i. On ER networks, the degree distribution is Poissonian (all moments finite), and flux maxima converge to Gumbel statistics. On scale-free networks with $\gamma \leq 3$, the diverging $\langle k^2\rangle$ implies that a non-negligible fraction of nodes experience heavy-tailed flux distributions, and

the maximum flux across the network follows Fréchet statistics with tail index controlled by γ [82].

Spectral properties. The mixing time $t_{\text{mix}} \sim 1/\lambda_2$ governs the temporal autocorrelation of node flux. A small spectral gap (as in scale-free networks) implies slow mixing and persistent correlations, violating the i.i.d. assumption of classical EVT. This leads to *clustering* of extreme events (multiple exceedances in close succession) and inflated estimates of return levels if i.i.d. EVT is naively applied. The *extremal index* $\theta \in (0, 1]$ quantifies the degree of clustering: $\theta = 1$ for independent exceedances and $\theta < 1$ for clustered ones [93].

Community structure. Networks with strong community structure exhibit heterogeneous flux distributions at the mesoscale: inter-community bridges carry systematically higher load and fluctuations than intra-community edges, modifying the spatial distribution of extreme events.

Multivariate and Spatial Extremes

In a network, extreme events rarely occur at a single node in isolation. The propagation of a cascade means that multiple nodes may simultaneously experience extreme flux. *Multivariate EVT* [94] characterises the joint tail behaviour of $(f_1, f_2, \ldots, f_N)$ and quantifies extreme dependence through the *spectral measure* or *tail dependence coefficient*. On networks, the joint tail distribution of neighbouring nodes is shaped by the transition probabilities and the network topology. Understanding spatial extremes is essential for predicting the extent of cascade events and for designing interventions that prevent multi-node overloads.

Non-Stationarity

Real transport networks are non-stationary: traffic demand follows daily and weekly cycles, and structural changes (node/edge additions, failures) alter the stationary distribution. *Non-stationary EVT* extends the GEV by allowing $\mu(t)$, $\sigma(t)$, and $\xi(t)$ to be functions of time or covariates [87]. In the context of networks, non-stationarity arises from time-varying walkers $W(t)$ or from temporal network structure; accounting for it requires careful covariate specification and likelihood-ratio model selection.

2.9.7 Connections to Network Failure

The extreme-event framework developed above connects directly to two failure mechanisms:

1. **Single-node overload.** When flux f_i exceeds capacity $C_i = (1+\alpha)\langle f_i \rangle$ (a special case of equation (2.16)), node i fails. The probability and return period of such events are given by equations (2.23) and (2.31), respectively.

2. **Cascading failure.** An initial extreme event at a hub redistributes load to neighbours, potentially triggering further exceedances in a cascade. The cascade size distribution can exhibit power-law tails [12, 95], a signature of criticality that EVT helps to quantify via the *self-exciting* point-process framework [96].

EVT thus provides a dual role: it characterises *individual* node failure probabilities (via marginal extreme-value distributions) and *systemic* risk (via multivariate extremes and spatial dependence measures).

2.9.8 Estimation and Inference in Practice

Maximum Likelihood Estimation

For a GEV-fitted block maxima sample $\{m_1, \ldots, m_B\}$, the log-likelihood is

$$\ell(\mu, \sigma, \xi) = -B \log \sigma - (1 + 1/\xi) \sum_{b=1}^{B} \log\left(1 + \xi \, \frac{m_b - \mu}{\sigma}\right) - \sum_{b=1}^{B} \left(1 + \xi \, \frac{m_b - \mu}{\sigma}\right)^{-1/\xi}, \quad (2.35)$$

maximised numerically (e.g. via Newton–Raphson or the Nelder–Mead algorithm). Standard errors and confidence intervals for return levels are obtained by the delta method or profile likelihood [87].

L-Moments

L-moments [97] provide robust, closed-form estimators for GEV parameters that are more stable than method-of-moments estimators, particularly in small samples or when ξ is close to -0.5. They are widely used in hydrology and are the preferred method in national flood-frequency estimation standards.

Bayesian EVT

A Bayesian approach assigns prior distributions to (μ, σ, ξ) and updates them via the likelihood, propagating parameter uncertainty directly into return-level credible intervals [87, 98]. This is particularly valuable in the network context, where the number of block maxima may be small (e.g. when studying rare node failures), and informative priors from physical reasoning (e.g. $\xi > 0$ for heavy-tailed flux) can stabilise inference.

2.9.9 Limitations and Challenges

Despite its generality, the application of EVT to network dynamics faces several challenges:

- **Dependence.** The i.i.d. assumption is violated by temporal and spatial correlations in network flux. The extremal index and mixing conditions must be verified, and dependent-data EVT must be employed when necessary [93].
- **Threshold selection.** In the POT method, the choice of u remains partly subjective and affects both bias and variance of estimates.
- **Finite-size effects.** Network flux distributions converge to their asymptotic forms slowly, especially for scale-free networks where $\langle k^2 \rangle$ diverges. Pre-asymptotic corrections are often significant for empirically relevant system sizes [82].
- **Non-stationarity.** Many real transport networks are strongly time-varying, and non-stationary EVT requires additional covariates that may be difficult to specify.
- **Multivariate complexity.** Joint extreme-value analysis of all N nodes is computationally intractable for large networks; dimension-reduction approaches (e.g. max-stable processes on graphs) are needed.

2.10 Conclusion

This chapter has surveyed the principal classes of dynamical processes studied on complex networks, providing the theoretical foundation for subsequent chapters. The key unifying message is that *network structure matters profoundly*: degree heterogeneity, spectral properties of the Laplacian and adjacency matrix, and community organization all qualitatively alter phase transitions, critical thresholds, and the statistics of fluctuations.

Specifically: the epidemic threshold vanishes in scale-free networks; synchronisability is controlled by the Laplacian spectral gap; cooperation is sustained by hubs through network reciprocity; and extreme transport events are amplified at high-degree nodes. The random-walk flux model provides a tractable framework for quantifying these effects, and its outputs feed directly into the Extreme Value Theory analysis.

Extreme Value Theory extends statistical analysis from the domain of typical fluctuations to the domain of rare, high-impact events. The Fisher–Tippett–Gnedenko theorem provides a universal characterisation of limiting extremal distributions: Gumbel for light-tailed, Fréchet for heavy-tailed, and Weibull for bounded parent distributions. The GEV unifies these three families into a single parametric model whose shape parameter ξ diagnoses the tail class. The POT/GPD approach provides an efficient inferential alternative using all exceedances above a high threshold.

When applied to complex networks, EVT reveals that heterogeneity in degree, spectral properties, and community structure shape the statistics of extreme events in fundamental ways. Scale-free networks, with their heavy-tailed degree distributions, exhibit Fréchet-type flux maxima, higher extreme-event probabilities, and power-law recurrence times. These findings form the theoretical foundation for the analyses of Chapters 3 onward, where EVT is combined with the random-walk flux model to characterise failure probabilities and cascade risks on complex networks. We do not explicitly use EVT, but only the *Peaks Over Threshold Method* as the algorithm to define extreme events.

Chapter 3

Network Failure Induced by Intrinsic Fluctuations

3.1 Introduction

Networked systems form the backbone of many modern infrastructures, including power grids, transportation systems, communication networks, and financial networks. The functioning of these systems relies on the ability of the network to transport flux—such as electricity, vehicles, information packets, or financial transactions—through its nodes and edges. A major concern in the study of such systems is the possibility of large-scale failures that disrupt their functionality.

Historically, studies of network failures have focused on externally induced perturbations such as random failures or targeted attacks on nodes or edges. For example, it is well known that scale-free networks are resilient to random failures but highly vulnerable to targeted attacks on hubs. Such behavior is often described as the "robust yet fragile" nature of complex networks.

However, in many real-world systems, failures can arise even in the absence of external perturbations. Instead, intrinsic fluctuations in the flux passing through the network can generate extreme events that trigger node failures. Examples of such phenomena include:

- Power grid failures triggered by fluctuations in load or frequency,

- Traffic jams arising from sudden increases in vehicular density,
- Packet congestion in communication networks.

In such cases, the network may gradually lose its ability to sustain normal operation as nodes begin to fail due to excessive load. The failure of a single node may redistribute its load to neighboring nodes, potentially causing further failures and triggering cascading events.

The aim of this chapter is to investigate how large intrinsic fluctuations in flux can lead to network failure. Specifically, we study networks in which flux is modeled using multiple random walkers. Extreme events correspond to instances where the number of walkers at a node exceeds a predefined threshold. When such events occur, the node is considered to have failed and is removed from the network.

We show that the approach to network failure follows a universal pattern characterized by three distinct regimes:

1. Independent node failures,
2. Cascade failures,
3. Overload failures.

These regimes are observed across several classes of networks, including Erdős–Rényi, scale-free, small-world, and lattice networks.

A networked system can fail when most of its components are unable to support flux through the nodes and edges. As studied earlier this scenario can be triggered by an external perturbation such as an intentional attack on nodes or for internal reasons such as due to malfunction of nodes. In either case, the asymptotic failure of the network is preceded by a cascade of nodal failures. In this chapter, we focus on the nodal failure arising from the intrinsic fluctuations in the flux passing through the nodes. By modeling these as extreme events, it is shown that three distinct nodal failure regimes can be identified before a complete network failure takes place. Further, the approach to network failure through the three regimes is shown to be qualitatively similar on a square lattice, all-to-all, scale free, and Erdos-Renyi networks. We obtain approximate analytical description of the approach to failure for an all-to-all network. This is also demonstrated numerically for real transportation network of flights and road networks.

It is well appreciated from our common experience that when networked systems fail, a large segment of population are affected and it unleashes significant economic losses. For instance, power grid failure or blackout [99] is one such example and, across the world, many large geographical regions have encountered power blackouts ranging from a few hours to even days. Heavy traffic jams on road networks, called grid locks, sometimes linger on several days. Excessive voice traffic in mobile phone network leads to many call drops. In all these examples, a functional network, upon the emergence of extreme events, loses its ability to support and facilitate normal flux and dynamics. A network is said to be resilient if it can resist the failures and resume its normal functions after a strong perturbation [100]. A study of such network failures and their resilience continues to attract research attention in a general setting of complex networks for more than two decades now [19, 24, 13, 101, 102, 103, 43].

The central question of interest is about how networks fail in response to perturbation, which can arise either due to external attacks or internal reasons [15, 14, 1]. Most of the earlier works had focussed on external attacks. For instance, it is known that scale-free networks display significant resilience to random attacks, but not against targeted attacks [5, 7]. Modeling studies in the specific context of the internet or in terms of its network analogues [6] have found a similar response to attacks, and this is type of resilience is dubbed "robust yet fragile" [104]. In networked systems, cascade of node failures can arise in response to failure of one or many nodes [12, 105, 13]. This typically happens in many critical infrastructure systems such as the power distribution network in which power blackouts are known to arise from uncontrolled cascading of nodal failures [12, 42, 106, 17, 107, 25, 108], in road networks as well in the form of spreading of traffic snarls [109, 110, 111], in connected devices or internet-of-things such as smart grids to even smart homes in which a cascade of undesired state changes can happen on devices [112]. Hence, an assessment of robustness or equivalently fragility of networks [16] is an important factor towards our understanding of network failures.

While externally induced attacks or perturbations have been well studied in the past, it is not yet well appreciated that *internal* fluctuations within a network can also be a source of instability that may ultimately lead to failure. In real systems, internal fluctuations arise from intrinsic stochastic nature of flux flowing between nodes. For instance, in power grid networks, as noted in the reports of blackouts [3], often fluctuations in current frequency beyond a tolerance threshold can induce cascading failure of transformers and culminate in

a blackout [113, 3]. In a road network, a sudden surge in vehicular traffic in the absence of any external factors can lead to cascading traffic jams across a road network.

In this chapter, we focus on extreme events caused by intrinsic fluctuations in a networked system and show the emergence of complete network failure starting from nodal failures. To study this in a general setting, we employ multiple random walkers to model "events" on networks. These walkers can be thought of as a flux of vehicles or packets of information passing through the nodes. Random walkers on networks and extreme events – a number of walkers meeting at a node purely by chance and a consequent breaching of threshold – had been well studied in the past [8, 10, 9, 21, 11, 114, 41]. The unusual feature of small degree nodes being more prone to extreme events in comparison to hubs was observed with standard and biased random walks on networks [8, 11]. Despite these results about intrinsic fluctuations and nodal extremes, how these fluctuations can lead to network failure remains unknown. We show two results; (i) Even without external perturbations, internal fluctuations can lead to complete network failure, and (ii) broadly, the network failure is approached through three distinct regimes independent of the finer details of the network.

3.2 Extreme Events on Complex Networks

3.2.1 Random Walk Dynamics on Networks

Consider a network consisting of N nodes and E edges. To model the flux through the network, we introduce W independent random walkers. Each walker moves from one node to a neighboring node at every discrete time step.

Let $w_i(t)$ denote the number of walkers at node i at time t. The distribution of walkers across the network evolves according to the rules of random walk dynamics.

For an unbiased random walk on an undirected network, the stationary probability that a walker occupies node i is proportional to the degree of the node:

$$p_i = \frac{k_i}{2E} \tag{3.1}$$

where k_i is the degree of node i.

This result follows from the detailed balance condition of random walk dynamics on networks.

3.3 Extreme events and network failure

Let us consider a complex network with N nodes, E edges, and W *independent* walkers executing random walk dynamics. Focussing on any one of its nodes (say, i-th node), the flux through this node is denoted by $w(t)$, the number of walkers at time $t = 1, 2, \ldots$. Then, the distribution of walkers is known to be a Binomial distribution given by

$$g(w) = \left(\begin{array}{c} W \\ w \end{array} \right) p^w \ (1-p)^{W-w}, \tag{3.2}$$

where $p = k/2E$ is the stationary occupation probability associated with the node that has degree k. Thus, $0 \leq w(t) \leq W$ would constitute an event at time t for our purposes. Then, an event at time $t = \tilde{t}$ would be designated as an extreme event if $w > \tau$, where τ is the threshold for identifying an event as extreme. In the presence case, τ is given by

$$\tau = \langle w \rangle + q \ \sigma_w, \tag{3.3}$$

where $\langle w \rangle$ and σ_w are the mean number of walkers and the associated standard deviation, and both depend on degree k of the node in question. For instance, if $q = 4$, then extreme events are those events occurring in the tail of $g(w)$ beyond $4\sigma_w$ from the mean. Then, the probability for the occurrence of extreme events, for fixed N and W, is given by

$$P(k) = \sum_{w=\lfloor \tau \rfloor}^{W} g(w) = I_p \left(\lfloor \tau \rfloor + 1, W - \lfloor \tau \rfloor \right), \tag{3.4}$$

where $\lfloor . \rfloor$ is the floor function, and $I_p(.,.)$ is the incomplete Beta function [115]. For a scale-free network, it is known that [8] occurrence probability of extreme events $P(k)$, in an average sense, is large for small k, and is small for hubs ($k \gg 1$).

Usually, extreme events tend to be catastrophic, and the affected nodes take finite time to recover, *i.e.*, relaxation is not instantaneous. For instance, traffic jams take a good amount of time to return to normal conditions, or defective transformers in a power distribution network cannot be replaced instantly (except if redundancy is built in to handle such situations). In the formalism leading to Eq. 3.4, it was implicitly assumed that the affected node $i_{\rm ee}$ can recover instantaneously after an extreme event. This is not true in practice. To understand the effect of nodal damage due to extreme events, we assume that the affected node $i_{\rm ee}$ cannot support the flux of walkers any more. The walkers left on $i_{\rm ee}$ at the time when extreme event

happens are re-distributed to the neighbouring nodes. After *every step* of random walk dynamics, additional three-step process is implemented on *every node* : (a) check for the occurrence of extreme event, (b) if extreme event had occurred, the affected node is disabled and walkers are redistributed to its immediate neighbours. This redistribution is done at the next time step to preserve the probability of the process. The affected node will not take part in the dynamics any more, (c) if extreme event did not occur, random walk dynamics is continued as before. As $t \to \infty$, more and more nodes are disabled due to extreme event occurrences, and the network ultimately loses the ability to support useful dynamics, at which point the network is said to have reached a "failed state". In some networks, a failed state might still be able to support trivial dynamics, *e.g.*, walk between just two surviving nodes. In this paper, we consider four different networks and study how this state of network failure is approached both as a function of time and as function of load-to-capacity ratio (defined below).

Distribution of Walkers at a Node

Since the walkers move independently, the number of walkers at node i follows a binomial distribution:

$$g(w) = \binom{W}{w} p^w (1-p)^{W-w} \tag{3.5}$$

where p represents the stationary occupation probability of the node.

The mean and variance of this distribution are given by

$$\langle w \rangle = Wp \tag{3.6}$$

$$\sigma_w^2 = Wp(1-p) \tag{3.7}$$

Thus, the instantaneous number of walkers at a node fluctuates around the mean value $\langle w \rangle$.

Definition of Extreme Events

An extreme event occurs when the number of walkers at a node exceeds a threshold value τ. The threshold is defined as

$$\tau = \langle w \rangle + q\sigma_w \tag{3.8}$$

where q is a parameter that determines how far into the tail of the distribution an event must lie to be considered extreme.

Typical values of q range between 3 and 4, corresponding to rare events in the tail of the distribution.

The probability of observing an extreme event at a node is

$$P(k) = \sum_{w=\lfloor \tau \rfloor}^{W} g(w) \tag{3.9}$$

which represents the probability that the number of walkers exceeds the threshold.

3.3.1 Model for Network Failure

In many real systems, nodes that experience extreme load cannot recover instantaneously. For example, a transformer that fails in a power grid may take hours or days to be replaced.

To incorporate this feature, we assume that when an extreme event occurs at a node, the node becomes permanently disabled.

The model evolves according to the following rules:

1. Random walkers move across the network according to random walk dynamics.
2. At each time step, the number of walkers at every node is recorded.
3. If the number of walkers at a node exceeds its threshold τ, an extreme event occurs.
4. The affected node is removed from the network.
5. Walkers present on the failed node are redistributed to neighboring nodes.

As nodes continue to fail over time, the network gradually loses its ability to support the dynamics of walkers.

The schematic diagram of the dynamics is represented in the figure 3.1.

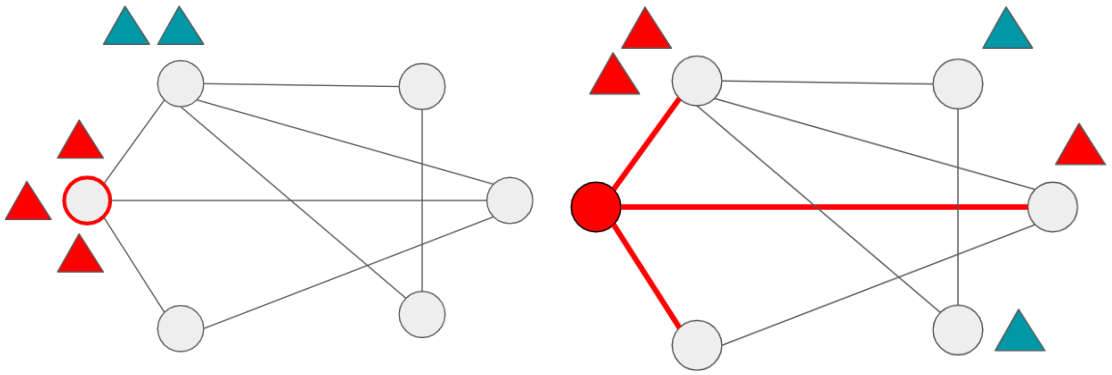


Figure 3.1: Schematic of node deletion and load redistribution. At (left) $T = 1$, the node in *red* has undergone extreme event, and in the (right) next time step $T = 2$, the edges(in red) are removed after distribution of its load to the neighbours. The walkers are coloured for better visualization, otherwise they're identical in nature.

3.3.2 Capacity–Load Ratio

To quantify the ability of the network to sustain flux, we define the network capacity as

$$C(t) = \sum_{i \in S_{ac}(t)} \tau_i \tag{3.10}$$

where $S_{ac}(t)$ represents the set of active nodes at time t.

The capacity–load ratio is defined as

$$\eta(t) = \frac{C(t)}{W} \tag{3.11}$$

where W is the total number of walkers in the system.

This ratio provides a measure of how close the network is to failure.

- $\eta > 1$: network operates safely

- $\eta \approx 1$: critical regime
- $\eta < 1$: overload regime

As nodes fail, the network capacity decreases and $\eta(t)$ gradually approaches zero.

3.4 Approach to network failure

3.4.1 All-to-all connected network

The central ideas will be illustrated using an all-to-all connected network, and subsequently for other types of networks. Consider an all-to-all network with $N = 100$ nodes on which $W = 9900$ walkers are executing random walk dynamics. In this work, we have kept the number of walkers $W = 2E$ for simplicity. At the initial time, all the walkers are placed randomly on any of the N nodes, and all the nodes begin to send/receive walkers. In our simulations, random initial condition for the walkers is achieved by placing all the walkers initially at an arbitrary node and then performing random walk for sufficiently long time. As random walk dynamics progresses, nodes begin to encounter extreme events. If an extreme event happens on i-th node at time t, then the node is rendered inactive and stands deleted. Hence, it cannot host random walkers anymore. Let $N_{ac}(t)$ and $N_{del}(t)$ represent, respectively, the cumulative number of active and deleted nodes on the network until time t. Then, $f_{ac}(t) = N_{\rm ac}(t)/N$ and $f_{\rm del}(t) = N_{\rm del}(t)/N$ represent the fractions of active and inactive nodes, such that $f_{\rm ac}(t) + f_{\rm del}(t) = 1$. It is useful to define instantaneous number of deleted nodes $n_{\rm del}(t)$ such that $N_{\rm del}(t) = \sum_{t'=1}^{t} n_{\rm del}(t')$. The corresponding instantaneous fraction is $F_{\rm del}(t) = n_{\rm del}(t)/N$.

Figure 3.2(a) displays $f_{\rm ac}(t)$ as a function of time for four different realization of random walk dynamics. Each realization corresponds to a different initial condition for walkers on the same network. As anticipated, $f_{ac}(t)$ tends monotonically towards zero. Two features can be inferred from this figure; initially, occurrences of extreme events tend to be few and hence $f_a(t)$ is nearly flat. After some time, the number of extreme events increases rapidly and $f_a(t)$ decreases rapidly and tends to zero. Ultimately, the network fails at time $t = T_{\rm fail}$. The failure time $T_{\rm fail}$ is stochastic, and is different for different realizations. Further, as shown in the inset of Fig. 3.2(a), $T_{\rm fail}$ depends on the value of threshold τ. In general, it is reasonable to anticipate that $T_{\rm fail}$ will be larger for larger τ, though this can be occasionally violated in specific realizations.

A more useful picture for the approach to network failure can be realized by eliminating time as follows. Let $C(t)$ be the capacity of the network defined as the maximum number of random walkers it can carry without breaching the node-dependent threshold (Eq. 3.3) on any of its active nodes. The total number of walkers on the network remains constant, but $C(t)$ keeps decreasing with every failure of a node. At the time of network failure, capacity of network to support walker flux becomes significantly small compared to the total number of walkers. This observation motivates us to define a parameter – capacity to load ratio – as

$$\eta(t) = \frac{C(t)}{W} = \frac{1}{W} \sum_{i \in \{S_{\rm ac}(t)\}} \tau_i, \tag{3.12}$$

in which the summation is over the set of active nodes $\{S_{\rm ac}(t)\}$ at time t. With temporal evolution, nodes get deleted due to extreme events, and network capacity $C(t)$ decreases, and consequently $\eta(t) \to 0$. In Fig. 3.2(b), instantaneous fraction of deleted nodes $F_{\rm del}(t)$ is shown as a function of $\eta(t)$ for several realizations. Unlike the temporal perspective in Fig. 3.2(a), remarkably, all the realizations collapse on the same (dotted) curve. Next, we obtain an approximate analytical description.

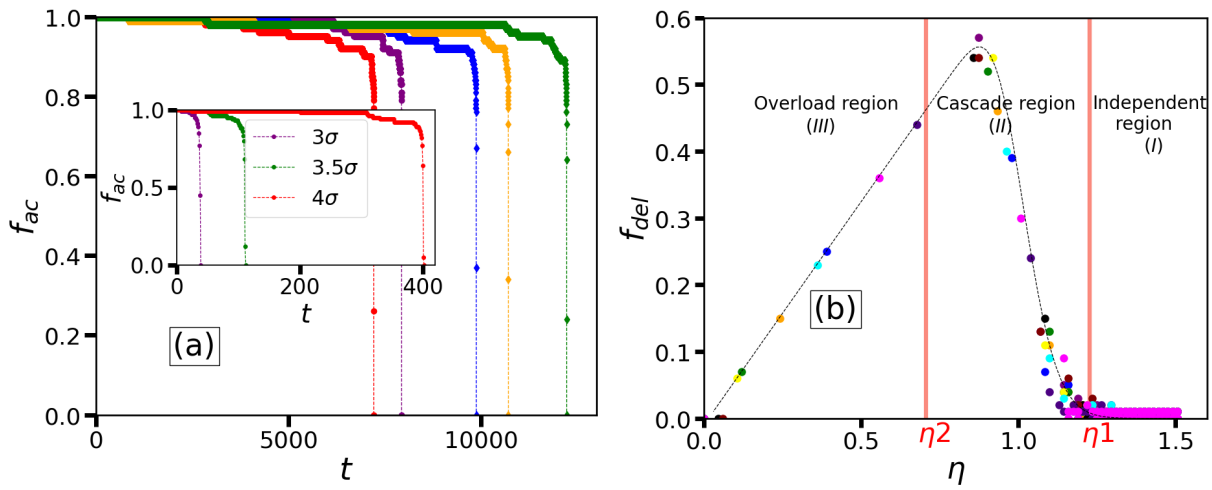


Figure 3.2: Approach to network failure on an all-to-all connected network. (a) fraction of active nodes $f_{\rm ac}(t)$ against time for 5 different realizations, and (b) instantaneous fraction of deleted nodes $F_{\rm del}(t)$ as a function of $\eta(t)$. The inset in (a) shows $f_{\rm ac}(t)$ for different threshold values (see Eq. 3.3) $\tau = \langle w \rangle + q\sigma_w$, with $q = 3.0, 3.5, 4.0$. The dotted curve in (b) is the analytical result in Eq. 3.16. Though failure time $T_{\rm fail}$ is different for each realization in (a), all of them collapse on the same (dotted) curve in (b). η_1 and η_2 represent boundaries between the regimes (see text for detailed description)

When a node encounters an extreme event, it is disconnected from the network. Consequently, other active nodes (even if they did not encounter an extreme event) may also lose one or more edges. At time instants when node failure happens, degree κ_i of i-th node changes while W remain unchanged. The diameter of this network being unity, immediately after the first node failure random walkers are spread over the entire network. Based on this assumption and Eq. 3.4, the probability $\phi_{\mathrm{del},i}$ of finding a walker on i-th node *after* N_{del} nodes have failed (and hence deleted from network) is

$$\phi_{\mathrm{del},i}(t) = \frac{\kappa_i(t)}{\sum_{j=1}^{N-N_{\mathrm{del}}(t)} \kappa_j(t)}, \tag{3.13}$$

where κ_i is the degree of i-th node after N_{del} nodes are deleted. Time-dependence in Eq. 3.13 arises because extreme events induce nodal failures and removal of edges during temporal evolution of walkers. For an all-to-all network, note that $\kappa_i = \kappa$ for all i. Hence, we suppress the index i. Thus, we have $\kappa_i(t) = \kappa(t) = N - 1 - N_{\mathrm{del}}(t)$. Using this in Eq. 3.13, we obtain a simplified form as

$$\phi_{\mathrm{del}}(t) = \frac{1}{N - N_{\mathrm{del}}(t)}. \tag{3.14}$$

Now, after N_{del} nodes are deleted, the probability for nodal failure (which equals the probability for the occurrence of extreme events) on any node can be obtained as

$$F(N_{\mathrm{del}}(t)) = I_{\phi_{\mathrm{del}}(t)} \left(\lfloor \tau \rfloor + 1, W - \lfloor \tau \rfloor \right). \tag{3.15}$$

The fraction of deleted nodes can be expressed as

$$F_{\mathrm{del}}(t) = N_{\mathrm{ac}}(t)\ F(N_{\mathrm{del}}(t)). \tag{3.16}$$

Now, we will track the approach to network failure by eliminating time in $F_{\mathrm{del}}(t)$ and $\eta(t)$. Note that both $F_{\mathrm{del}}(t)$ and $\eta(t)$ change only at time instants when extreme event occurs anywhere on the network. Figure 3.2(b) displays $F_{\mathrm{del}}(t)$ (solid line) as a function of $\eta(t)$. The simulation results from random walk realizations are shown as colored symbols. An excellent agreement between Eq. 3.16 and the simulation results are observed. This also allows us to clearly identify three distinct regimes as the complete network failure is approached on a timescale of T_{fail}. These regimes (described below) are separated by vertical lines in Fig. 3.2(b), and are discussed in detail below.

Independent node failures : First of these is the regime of independent node failures in which

failure of one node does not influence the other nodes to fail. Typically, at most, one node fails at a given time, and the time interval Δt between two consecutive node failures is large; $\Delta t >> 1$. These imply that node failures tend to be rare, and do not disturb the network function. Based on Eq. 3.12, let $\eta_{\max} = \eta(t = 0)$ be the maximum value of η for a given network configuration. Then, this regime begins $\eta = \eta_{\max}$ and breaks down at $\eta = \eta_1$ when the condition

$$\left| \left\langle \frac{dF_{\rm del}}{d\eta} \right\rangle \right| > 0 \tag{3.17}$$

is satisfied for the first time (see Fig. 3.2). In this, $\langle . \rangle$ represents an average over time interval δt such that $1 < \delta t \ll T_{\rm fail}$. In Fig. 3.2(b), this condition is satisfied for $\eta = \eta_1$, and it is marked by a vertical line. The independent node failure regime lasts until $\eta > \eta_1$ and is indicated as region I in Fig. 3.2(b).

Cascade failures : In this regime, as η decreases below η_2 colorred or η_1, the number of deleted nodes per time step is now more than 1, *i.e.*, $F_{\rm del} > 1$. The node failures in this regime are not independent since one node failure leads many other nodes to fail. In some parts of this regime, the total capacity is more than the total load present on the network ($\eta > 1$), but some of the nodes encounter extreme events (and get disabled) due to excess load received from the redistribution of walkers. In an all-to-all network, all the nodes are neighbors of each other and hence, these failures are correlated with one another. Failure of a small number of nodes is followed by the failure of a larger number of nodes at the next time step. Such a sequence of node failures is called the cascade failures, and this regime lasts until $\eta = \eta_2$, where η_2 is determined through an empirical relation $\eta_2 = \alpha \eta_{\max}$. In this, $\eta_{\max}$ is the value of η at which $F_{\rm del}$ is maximum, and $\alpha = 0.8$. This cascade failure regime is indicated as Region II in Fig. 3.2(b). The transition from independent to cascade failure regime becomes sharper as the threshold τ is increased.

Overload failure : In this regime, the entire network fails with deletion of all the remaining nodes in one time step, or in no more than 2 time steps. In this case, as it is a one-step failure, number of deleted nodes equals the instantaneous number of active nodes, and total load on the network is greater than its carrying capacity, *i.e.*, $\eta << 1$. As a consequence, each node is already overloaded, and typically it takes no more than one time step for all the nodes to fail together. This is evident in the region $\eta < \eta_2$ (shown as Region III in Fig. 3.2(b)) since for each realization of the random walk dynamics there is just one data point appearing in this regime.

Compared to the temporal picture shown in Fig. 3.2(a), an elegant characterization of the approach towards network failure – triggered by the intrinsic fluctuations in flux – emerges when the same data is examined as a function of η as displayed in 3.2(b). In particular, the analytical result in Eq. 3.16 provides a good description of the simulation results and helps to identify three distinct regimes. The next natural question is to ask if these three regimes occur in other types of network as well. We address this question below. The η_1 is obtained by taking the running averages of the multiple realizations in a particular network and estimating the change in slope over a period of capacity-to-load variation. The η_2 is estimated considering 0.8 times the peak fraction of deletion experienced by a particular network. This particular value is obtained by considering multiple different initial points inside the cascade regime. These values give a good overview of the phases of the network that can also be visualized for synthetic and real-world networks.

To investigate the generality of the above results, we performed simulations on several network models.

This type of analysis is possible for Cayley tree for the initial step. With every node deletion, the network continue to loose symmetry and it fragments with different loads. This load fragmentation is not proportionate to the fragmented Cayley tree. The brief details of calculations is shown below:
Although the simulation can be applied directly without modification, the analytical simplifications cannot be. The analytical solution Eq. 5-7 was dependent on the simplification that when N_{del} nodes fail, the *remaining active network* is still all to all, as every active node still has the same degree, $k(t) = N - 1 - N_{del}$.

This is not true for a Cayley tree. When a node fails, the network fragments and splits into k disconnected branches. The k neighbours of the failed node have their degree $k-1$, and other nodes still have degree k. As the network loses its regularity, we cannot use the simplified Eq.5:

$$\phi_{del,i}(t) = \frac{k_i(t)}{\Sigma_{j \in S_{ac}(t)} k_j(t)}$$

This value varies as some nodes have degree k, while others which have their neighbours deleted have degrees $k-1, k-2$ etc. This phenomenon increases as more and more nodes experience extreme events. Similarly, the failure probability of a node becomes unique for each active node i,

$$F_i(t) = I_{\phi_{del,i}(t)(\lfloor q \rfloor)+1, W-\lfloor q \rfloor}.$$

We *can* calculate the extreme event probability analytically at $t = 1$ though, as then the network is in its initial undisturbed state. If we apply Eq. 4 to the initial state, we get

$$\phi_{del,i}(t = 0) = \frac{k_i(t = 0)}{\Sigma_{j \in S_{ac}(t=0)} k_j(t = 0)}.$$

At $t = 0$, every node has degree $k_i = k$, so $\Sigma k_j = N \times k$. Hence the stationary probability, $p = \frac{k}{N \times k} = \frac{1}{N}$.

Now the flux w is the sum of W independent random walks, given by Binomial distribution,

$$P(w) = \binom{W}{w} p^w (1 - p)^{W-w},$$

where $p = \frac{1}{N}$. Thus, the probability of extreme events $F_i(t = 1) = \Sigma_{w=q_{thresh}+1}^{W} P(w)$. Then, similar to the all-to-all case, we have

$$F_i(t = 1) = I_p(q_{thresh} + 1, W = q_{thresh}).$$

Here $q_{thresh} = \lfloor \tau \rfloor$. The single value $F_i(t = 1)$ is the analytical probability that any specific node will fail at $t = 1$, since all nodes are identical at this stage. Based on the methodology used by us, analytical calculation is no longer feasible after deletion of the first node. After one node fails, the network becomes heterogeneous, with at least 2 distinct types of nodes: k neighbours of the failed node and the $N - 1 - k$ non neighbour. Now, the total degree becomes $\Sigma k_j = (k \times (k - 1)) + ((N - 1 - k) \times k) = k(N - 2)$. Also, we have ignored the "extra walkers" in the network due to deletion and redistribution. The new occupation probabilities are

$$p_{neighbour} = \frac{k - 1}{k(N - 2)}$$

and

$$p_{others} = \frac{k}{k(N - 2)} = \frac{1}{N - 2}.$$

Thus, now for every new "block" we have to re-estimate the probabilities at each time step after node deletion happens. As shown in Fig. 3.3, left figure shows fraction of active nodes f_{ac} as a function of time, for two initial conditions. There's no definite regime present, this can be attributed to the limited short range connectivity, as the network forms disconnected blocks before load can be distributed effectively. The network attains a fragmented steady state (with isolated nodes) when 20% of the network remains active. In Fig. 3.3, right figure

shows the fraction of deleted nodes F_{del} as a function of capacity-to-load ratio η. Here we can see that node deletions per step are a small fraction of the network and the nature of the plot indicates that they qualitatively fall in the independent failures regime.

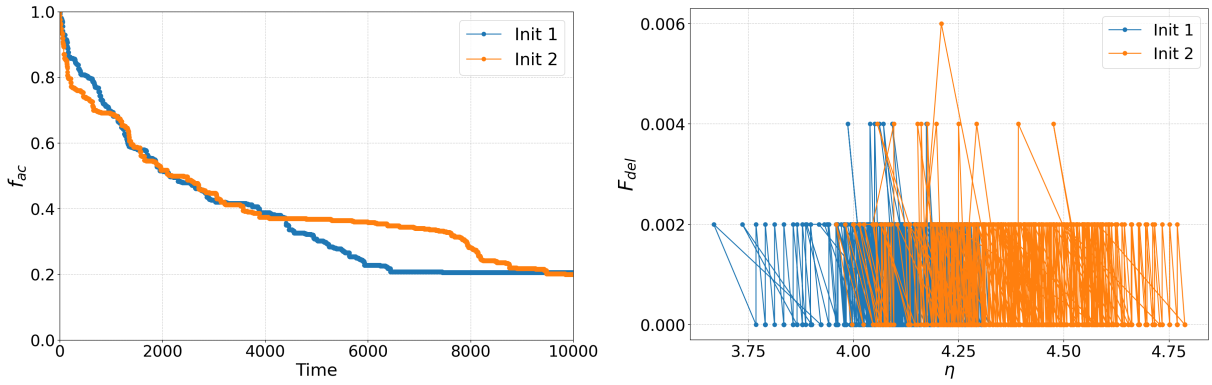


Figure 3.3: Dynamics for Cayley tree of size 500, having average degree 6. (left) depicts the fraction of active nodes as a function of time, (right) shows the fraction of deleted nodes as a function of η. There are two different initializations shown in the figures.

3.4.2 Effect of Network topology: ER, BA and Small World networks

In this subsection, we examine the approach to network failure in Erdos-Renyi (ER), Barabasi-Albert (BA), and small world (SW) networks. The simulation results for all the three types of networks are depicted in Fig. 3.4. These networks are generated using `NetworkX` [116]. We employ an Erdos-Renyi network with $N = 2000$ nodes and $E = 10028$ edges and diameter $d_{er} = 6$, a small-world network with $N = 2000$ and $E = 60000$ and $d_{sw} = 4$, Barabasi-Albert network with $N = 5000$ and $E = 19915$ and $d_{ba} = 6$, and lastly a square lattice. Random walk simulations for T timesteps are performed with $W = 2\,E$ walkers whose initial positions at time $t = 0$ are randomly chosen. Before extreme events are monitored, 5000 time steps of random walk are ignored to ensure that steady state is reached.

The broad features of the approach to network failure as a function of time (Fig. 3.4(a-c)) and with η (Fig. 3.4(d-f)) are qualitatively similar to that observed in all-to-all network in Fig. 3.2. Hence, it can be stated that approach to network failure – induced by intrinsically generated extreme events – is qualitatively similar for ER, BA and SW networks. In particular, the three regimes identified and described for all-in-all case hold good in Fig. 3.4(d-f)

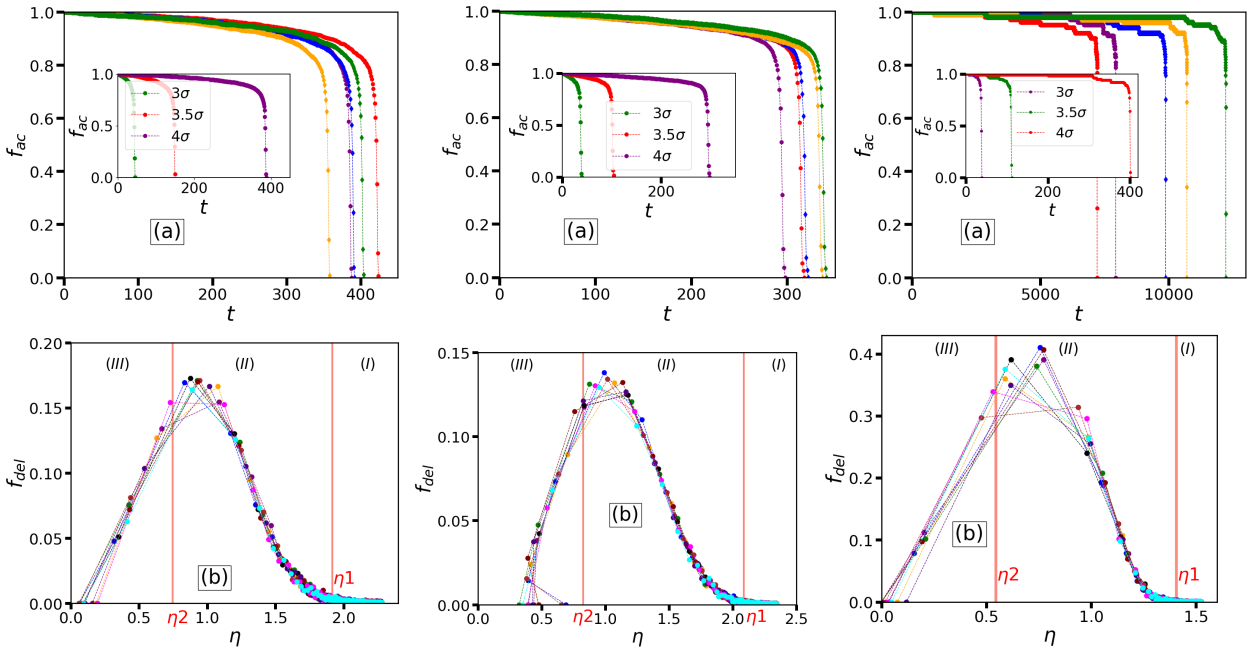


Figure 3.4: Approach to network failure is depicted as a function of time and η. Fraction of active nodes as a function of time (top), and instantaneous fraction of deleted nodes as a function of η (bottom) for $q = 4$. Approach to failure due to extreme events on (a,b)(left) Erdos-Renyi network with $\eta_{max} = 2.28$, (a,b)(middle) Barabasi-Albert network with $\eta_{max} = 2.35$, and (a,b)(right) small world network with $\eta_{max} = 1.52$. The insets in (a,c,d) shows three cases for different threshold values. In (b,d,f), η_1 and η_2 demarcate the boundaries between the three regimes – independent failure regime [indicated as (I)], cascade regime [indicated as (II)], and overload regime [indicated as (III)]. See text for details about how η_1 and η_2 are determined.

as well. The vertical lines shown in Figs. 3.4(d-f) demarcate the independent, cascade and overload regimes of network failure. Further, as $t \to \infty$, the size of the largest connected component L (not shown here) tends to zero or a small number indicating that network has effectively lost its functional capability to process flux.

Despite the broad similarity of the features in Fig. 3.4 to that in Fig. 3.2, there are differences arising from the nature of connectivity in the networks other than all to all. For instance, in these networks, as $t \to \infty$, nodes get isolated from the bulk of the network with walkers trapped in those nodes. The fraction of nodes getting isolated may differ in different realizations and different networks. Isolated nodes are essentially inactive nodes, and the $W_{\rm trap}$ trapped walkers on them cannot perform any dynamics. The effective number of walkers is $W_{\rm eff} = W - W_{\rm trap}$. This situation can arise even if a node does not encounter extreme events. Hence, due to this, both capacity and load are decreasing but rate of decrease differ depending upon the network topology. For instance, in BA network, the rate of decrease in load $W_{\rm eff}$ is faster than that of capacity C. Thus, the ratio $\eta(t) = C(t)/W_{\rm eff}$ increases, and consequently the network shows an inclination to return to the independent regime. This effect is visible in Fig. 3.4(d), and this becomes more pronounced as threshold τ increases. Further, maximum fraction of nodes deleted at a single step depends on the diameter of the network – shorter the diameter more number of nodes are deleted. Hence, it is highest in an all-to-all network. This can be inferred by comparing the peak values in Fig. 3.4(b,d,f).

Next, we consider a square lattice network with $N = 2500$ nodes and $E = 4900$ edges. The random walk simulations were performed with $W = 2\,E$ walkers and the results are displayed in Fig. 3.5. The decay of the fraction of active nodes f_{ac} as a function of time is shown in Fig. 3.5(top) for a few realizations. Unlike similar results shown for the case of heterogeneous networks in Fig. 3.4, f_{ac} displays nearly the same decay profile in every realization. Further, notice that f_{ac} never reaches zero but saturates at $f_{ac} \approx 0.15$. This happens because, as $t \to \infty$, a very small number of connected nodes, often in different clusters, tend to survive and support dynamics though the network as a whole has effectively failed and cannot support dynamics.

Figure 3.5 shows the fraction of inactive nodes $F_{\rm del}$ as a function of η.

As in other heterogeneous networks discussed earlier, the three failure regimes can still be identified; however, the underlying topology of the square lattice leads to important

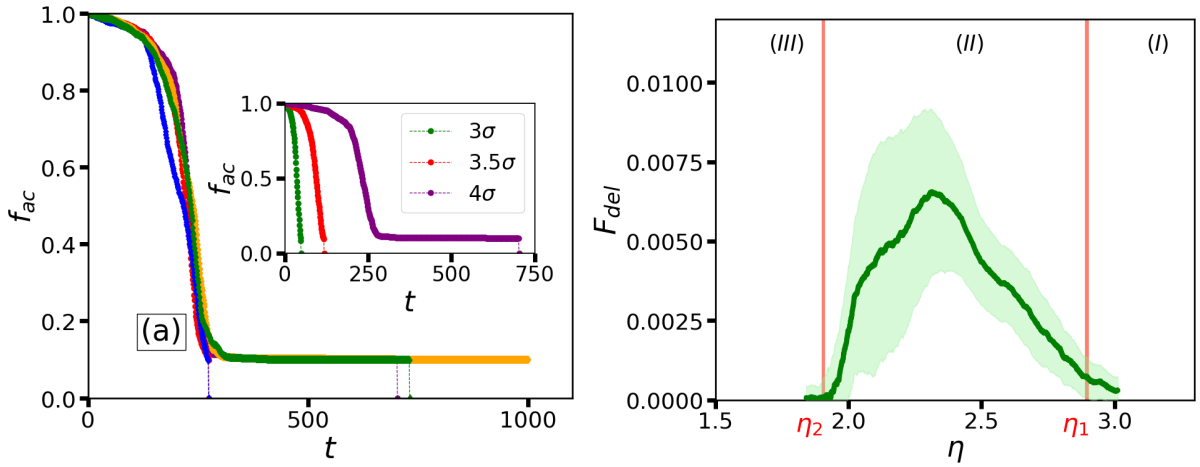


Figure 3.5: Approach to network failure on a square lattice. (left) depicts the fraction of active nodes as a function of time, (right) shows the fraction of deleted nodes as a function of η for $q = 4$. η_1 and η_2 represent boundaries between the regimes and $\eta_{max} = 3.02$. The solid line is the running average $\langle F_{\rm del}(\eta)\rangle$ over 10 initial conditions. The light green band shows the standard deviation $\sigma_{F_{del}}(\eta)$ within a fixed window of $\Delta\eta = 0.1$.

qualitative differences. In a square lattice, node failures are not strictly independent, since the absence of long-range connections and the resulting large network diameter confine the redistribution of load to local neighborhoods. Each node has a maximum degree of four, and therefore the failure of a node is accompanied by the removal of at most four edges. The load carried by the failed node is consequently transferred only to its immediate neighbors, which are themselves topographically adjacent. This local redistribution leads to a progressive acceleration in the rate of node deletion as failures spread across the lattice. The deletion rate reaches a maximum when the cascade spans a large fraction of the network and boundary nodes also begin to fail. In contrast to well-connected networks studied earlier, where long-range connectivity enables rapid global load sharing, the square lattice lacks such pathways. As a result, walkers accumulate locally, leading to a rapid build-up of load in confined regions. This enhances the probability of extreme events and drives the system into the cascade regime. However, unlike in well-connected networks, these cascades remain spatially localized and are comparatively smaller in extent. As the dynamics progresses further, the rate of deletion slows down due to extensive fragmentation of the network. A large number of isolated nodes and small disconnected clusters are formed, each supporting only a limited amount of load. Consequently, there is no distinct global overload failure regime. Instead, residual activity persists within these disconnected components until the end of the simulation. Although the square lattice loses most of its nodes and edges, a few disconnected

clusters survive for very long times and may never fail. At this stage, the network has effectively ceased to support meaningful transport or collective dynamics.

3.4.3 Real-World Network: Flight Network

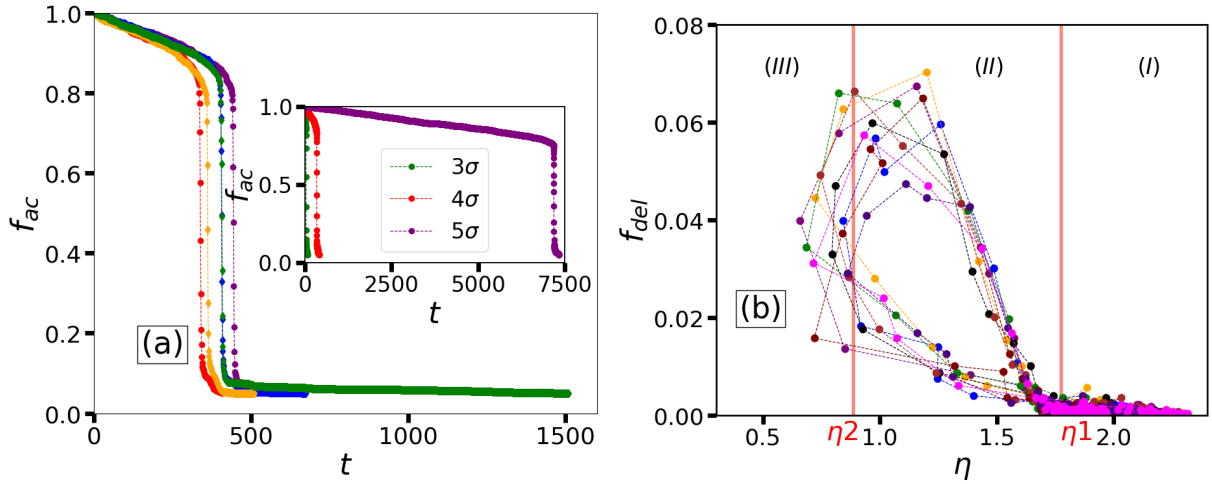


Figure 3.6: Approach to network failure for a flight network. (left) the fraction of active nodes as function of time. (right) the fraction of deleted nodes against η. η_1 and η_2 represent boundaries between the three regimes, also $\eta_{max} = 1.96$. Due to significant fraction of trapped walkers for $\eta < 1$, overload regime is marked by a strong tendency to return to independent regime.

We apply the idea of network failure to a flight network with $N = 2789$ nodes, $E = 14795$ edges, and diameter $d_{\text{fl}} = 14$. The dataset was obtained from the Network Repository [117]. This network is of "Barabasi-Albert" type, and differs from synthetic networks due to its large diameter $d_{\text{fl}} = 14$, compared to $d_{\text{ba}} = 6$ for a Barabasi-Albert network of similar size. As before, we obtain the decay of active nodes f_{ac} as a function of time for a few realizations. Here, the decay profile (Fig. 3.6(left)) is similar to that of a scale free network, but a new steady state forms after the "cascading" failure regime where most of the network has failed. However, due to the formation of disconnected segments the dynamics continues for a considerable amount of time. The network fragments, and has isolated segments which continue to support dynamics. Hence, due to trapped walkers (similar to scale-free network), a return to the independent failure regime is observed for $t \gg 1$ in Fig. 3.6(bottom).

Road networks embedded in 2D space have a structure similar to a regular graph or Cayley tree. Hence the dynamics are very similar to these (already discussed) graphs, with additional features. Since we were focussing on the networks which qualitatively show three regime

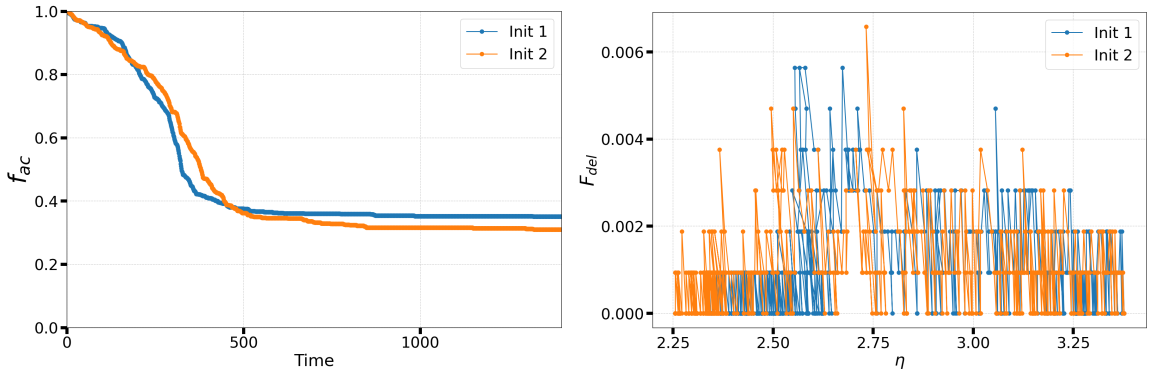


Figure 3.7: Dynamics for Ahmedabad road network with 1064 nodes, and having 1528 edges. (left) depicts the fraction of active nodes as a function of time, (right) shows the fraction of deleted nodes as a function of η. There are two different initializations shown in the figures.

failure, there will be additional features to these three regimes which depend on the detailed network structure. The Ahmedabad road network was obtained using geographic data from Google Maps [118], which was subsequently converted into a graph representation (edge list) for network analysis. The Fig. 3.7 left, shows fraction of active nodes as a function of time, it's similar to Cayley tree case, where there is a gradual node deletion and network attains steady state (with isolated nodes) at around 30% of the total network size. The network has limited connectivity and only short range connections exist among the nodes. Thus load distribution is inefficient. Thus in Fig. 3.7 right, we find that the deletion per step is a small fraction of the network, and it resembles independent regime qualitatively.

Table 3.1: Network regions

Network	$\eta 1$	Peak	$\eta 2$
All to all	1.23	0.88	0.70
Erdos-Renyii	1.92	0.94	0.75
Small world	1.40	0.69	0.55
Barabasi-Albert	2.09	1.04	0.83
Square lattice	2.9	2.33	1.9
Flight	1.78	1.12	0.89

In conclusion, we studied the network failures induced by large intrinsic fluctuations in the flux of random walkers modelled as extreme events, devoid of any external stimulus. While network failures from external perturbations are well studied [99, 24, 119], we demonstrate that intrinsic fluctuations alone can lead to network collapse. Crucially, failure proceeds

through three regimes: (i) uncorrelated failures, (ii) cascading collapses, and (iii) overload (one-step failure) regime. These regimes emerge across diverse networks and are analytically described for all-to-all networks (Eq. 3.16), matching well with simulations. The results challenge the paradigm that resilience requires only protection against external shocks. Instead, internal fluctuations – ubiquitous in power grids, traffic, and communication systems – require new mitigation strategies. While we assumed permanently failed nodes, real systems often allow recovery. Future work could extend this framework by introducing repair dynamics to explore resilience in more realistic settings.

3.5 Summary

It is known that external perturbations lead to failure of network as a whole, and this scenario had been extensively studied earlier [99, 24, 119]. For instance, power blackouts are examples of network failure originating from a possible technical fault in one transformer on the network. In contrast, in this chapter, we study network failures induced by large intrinsic fluctuations in the flux and not due to any external reasons. Then, a relevant question of interest is how network failure is approached as a result of extreme fluctuations. To answer this question, we considered networks on which flux is modelled by the dynamics of multiple random walkers. In this scenario, the "events" will be the instantaneous number of walkers $w(t)$ on a node at time t, which is stochastic in nature. Then, extreme events in $w(t)$ will correspond to pronounced deviations from its mean behaviour. This defines extreme event on a node and leads to nodal failure. To study network failure, the node that encounters extreme event is disabled, and the walkers (load) on it are transferred to neighbouring nodes. Thus, as more nodes are disabled due to extreme events, ultimately network is unable to support dynamics.

We show that approach to network failure can be characterized by studying number of node failures, not as a function of time but as function of parameter η, the ratio of load to capacity of the network. Then, for several popular types of networks considered in this chapter, it can be seen that approach to network failure follows a similar pattern, as observed in Fig. 3.4(b), with three distinct regimes. Firstly, there is a regime of uncorrelated network failures with long inter-event time intervals. Second is the regime of cascades, in which one node failure triggers many others. Third, is the regime of overload failures in which remaining nodes fail within 1-2 time steps. We have shown that all the networks considered in this chapter pass through these three regimes before the entire network fails. For the case

of all-to-all connected network, we obtain an analytical function Eq. 3.16 that describes approach to network failure, which is also in good agreement with simulations. Thus, the main message from this work is that, even in the absence of external perturbations, large intrinsic fluctuations alone can make a network dysfunctional.

In this chapter, we have assumed that a failed node never recovers. This is contrary to what happens in realistic situations. Hence, in future, it will be interesting to study how some of these results presented here will change if nodal repair times T_r are introduced. This implies that a failed node can recover after a timescale of T_r, and in principle this timescale could be stochastic as well. The main conclusions in the chapter about route to network failure can be tested in realistic scenarios.

Chapter 4

Repair on Networks

Complex networks — from power grids and communication systems to biological pathways and financial webs — operate under persistent perturbations. While a large body of work has characterized how networks fail, the complementary process of *repair and recovery* remains comparatively underexplored. This chapter addresses both sides of that gap.

First section develops the theoretical foundations: failure taxonomies, conceptual repair frameworks, local and global repair strategies, stochastic models, topology-dependent efficiency, and metrics of resilience.

Next section analyses repair dynamics in networks driven by *intrinsic* load fluctuations. Starting from a microscopic random-walk model, we derive a coarse-grained delay differential equation, characterize the critical repair delay, and identify structural signatures that precede network collapse.

4.1 Theoretical Foundations

Complex networks have emerged as a powerful paradigm for modelling interconnected systems with non-trivial topology and heterogeneous interactions. A central theme in network science is understanding how such systems respond to failures, whether random or targeted.

Historically, research has focused on *robustness* — the ability of a network to maintain functionality under perturbations. However, real-world systems rarely remain static after failure. Instead, they exhibit adaptive behaviour through *repair*, *recovery*, or *reconfiguration*.

Power grids reroute flows after outages, biological systems regenerate damaged components, and communication networks dynamically adjust routing protocols.

Repair processes are inherently dynamic and often interact with the underlying network topology. Unlike failure processes, which degrade network structure, repair aims to restore connectivity, functionality, or performance. The study of repair is therefore central to understanding *resilience* — the ability of a system to absorb disturbances and recover.

4.2 Failure Mechanisms

Let $G(V, E)$ denote a network with node set V and edge set E. Failures in nodes or edges are broadly classified as:

- **Random failures:** nodes or edges are removed uniformly at random.
- **Targeted attacks:** high-degree or high-betweenness nodes are preferentially removed.
- **Cascading failures:** failures propagate through load redistribution or dynamical coupling.

The key structural observable is the size of the giant connected component (GCC), S, which serves as a proxy for network functionality. In percolation theory, a critical threshold p_c marks the fraction of removed nodes beyond which S collapses discontinuously.

Cascading failures introduce additional complexity. In a load-based model, each node i carries load L_i and has capacity $C_i = (1 + \alpha)L_i$, where α is a tolerance parameter. When a node fails, its load is redistributed, potentially triggering further failures. Repair mechanisms must therefore counteract both structural damage *and* dynamical cascades.

4.3 Conceptual Framework for Repair

Repair in networks is any process that restores functionality after damage. We distinguish three complementary aspects.

4.3.1 Structural vs. Functional Repair

Structural repair restores network topology by re-adding nodes or edges, rewiring connections, or introducing redundancy. *Functional repair* restores dynamical processes — load

redistribution, flow rerouting, control interventions — without necessarily reconstructing the original topology.

4.3.2 Temporal Aspects

Let τ_f and τ_r denote characteristic timescales of failure and repair, respectively. The ratio

$$\eta = \frac{\tau_r}{\tau_f} \tag{4.1}$$

plays a decisive role: $\gamma \approx 1$ corresponds to fast repair that can keep pace with failures, while $\gamma \gg 1$ implies that repair lags far behind, allowing cascades to develop unchecked. Repair may be instantaneous (idealised) or *delayed*, introducing a competition between failure and recovery timescales that is a central theme of Part II.

4.4 Local Repair Mechanisms

Local repair relies on information available at individual nodes or their immediate neighbourhood.

4.4.1 Nearest-Neighbour Rewiring

When node i loses edge (i, j), it forms a new edge (i, k) where k is chosen from neighbours of j or from nodes within a specified radius. This preserves degree while altering topology, tending to preserve clustering and reduce path-length degradation.

4.4.2 Self-Healing Networks

Self-healing models allow nodes to reconnect autonomously. A common rule is

$$P_{ij} \propto e^{-d_{ij}/\xi}, \tag{4.2}$$

where d_{ij} is the physical distance and ξ a characteristic length scale. Such models are particularly relevant for wireless sensor networks.

4.4.3 Redundant-Link Activation

Some networks contain dormant edges that are activated upon failure. This mechanism enhances robustness without continuous operational cost, providing resilience reserves that are utilised only when needed.

4.5 Global Repair Strategies

Global repair uses system-wide information and optimisation.

4.5.1 Optimisation-Based Restoration

Given a damaged network, one may solve

$$\max_{E'} \; S(G') \tag{4.3}$$

subject to a budget constraint on the number of edges added. This is generally NP-hard; practical approaches include greedy algorithms, simulated annealing, and genetic algorithms.

4.5.2 Flow-Based and Centralised Repair

In infrastructure networks, repair aims to restore flow. For power grids, optimal power flow (OPF) problems are solved after failures to determine feasible operating points. In communication networks, centralised protocols reroute traffic globally to bypass congested or failed nodes.

4.6 Stochastic Models of Repair

Repair processes are inherently stochastic. A foundational model treats each node as a two-state system:

$$\text{Failure:} \quad A \to F \quad \text{with rate } \lambda, \tag{4.4}$$

$$\text{Repair:} \quad F \to A \quad \text{with rate } \mu. \tag{4.5}$$

The mean-field evolution of the active fraction x is

$$\frac{dx}{dt} = -\lambda x + \mu(1 - x), \tag{4.6}$$

giving steady state $x^* = \mu/(\lambda + \mu)$.

4.6.1 Networked Failure Processes

In a network, failure rates depend on the state of neighbours:

$$\lambda_i = \lambda_0 + \beta \sum_j A_{ij}(1 - x_j), \tag{4.7}$$

where A_{ij} is the adjacency matrix. This coupling introduces phase transitions between globally active and collapsed states, analogous to epidemic spreading above the epidemic threshold.

4.7 Cascading Failures and Repair

Let $f(t)$ denote the fraction of failed nodes. A simple competition model is

$$\frac{df}{dt} = F(f) - \mu f, \tag{4.8}$$

where $F(f)$ captures cascade amplification. When μ is large, repair suppresses the cascade; when μ is small, global collapse may occur.

Repaired nodes re-enter the system either with reset load or with residual damage — the choice significantly affects long-term stability and the probability of secondary cascades.

4.8 Topology-Dependent Repair Efficiency

The effectiveness of repair depends strongly on network structure.

- **Erdős–Rényi networks:** homogeneous degree distribution leads to uniform repair effects; percolation thresholds are well-defined.
- **Scale-free networks:** hubs are critical. Targeted repair of high-degree nodes is highly effective, while random repair is comparatively inefficient.

- **Small-world networks:** short path lengths facilitate rapid recovery propagation, but clustering may trap failures locally.

4.9 Adaptive and Co-evolving Networks

In many real systems, network structure evolves alongside dynamics. An adaptive rewiring rule

$$(i, j) \to (i, k) \quad \text{if } j \text{ is failed} \tag{4.9}$$

can lead to phase transitions between a connected active phase and a fragmented phase. More generally, co-evolutionary dynamics,

$$\dot{x}_i = f(x_i, \{x_j\}) \,, \tag{4.10}$$

$$\dot{A}_{ij} = g(A_{ij}, x_i, x_j) \,, \tag{4.11}$$

allow state and topology to influence each other — highly relevant for social and biological systems.

4.10 Metrics for Repair Efficiency and Resilience

Key metrics for evaluating repair strategies include recovery time, fraction of functionality restored, and repair cost. A global resilience measure is the time-integrated functionality:

$$R = \frac{1}{T} \int_0^T S(t)\, dt, \tag{4.12}$$

which balances both the depth of damage and the speed of recovery. Optimal repair strategies must trade off speed, cost, and robustness; control-theoretic tools such as feedback control and model predictive control provide a formal framework for this optimisation.

4.11 Effect of Repair on Flux-Driven Networks

The assumption that nodes experiencing extreme events (EE) are permanently deleted provides a worst-case boundary for network vulnerability. However, physical infrastructure and biochemical pathways frequently possess intrinsic relaxation or repair mechanisms. Introducing a finite cool-down period transforms the network from a system undergoing monotonic

degradation to one capable of sustaining non-equilibrium steady states and oscillatory phase transitions.

Here we study the stability of networks driven by random-walker flux — a setting where failures arise from *intrinsic* fluctuations rather than external shocks. The core question is: *Can repair mechanisms stabilise a network against internally arising extreme events, and if so, what are the conditions?*

4.11.1 Flux-Driven Failure

Chapter 3 was dedicated purely on this.

4.11.2 State-Dependent Failure Rate

Let $x(t)$ be the fraction of active nodes. As nodes fail, the load redistributes to the survivors, so the effective occupation probability becomes

$$p(x) = \frac{1}{Nx}. \tag{4.13}$$

The failure flux is therefore state-dependent:

$$F_{\mathrm{del}}(x) = xN \cdot P_{\mathrm{EE}}(x). \tag{4.14}$$

4.11.3 Deterministic Evolution with Delayed Repair

Without repair the fraction of active nodes obeys

$$\frac{dx}{dt} = -x\, P_{\mathrm{EE}}(x). \tag{4.15}$$

The nonlinear amplification of $P_{\mathrm{EE}}(x)$ as x decreases drives a positive-feedback cascade: small initial failures increase the load on survivors, which raises P_{EE}, which induces further failures.

Introducing repair in which a failed node is restored after a delay τ_R gives the delay differential equation (DDE)

$$\frac{dx}{dt} = -x\, P_{\mathrm{EE}}(x) + \frac{1}{\tau_R}\big[1 - x(t - \tau_R)\big]. \tag{4.16}$$

The repair term supplies memory: nodes that failed at time $t - \tau_R$ are reintroduced at time t. At steady state equation (4.16) gives

$$x^* \, P_{\mathrm{EE}}(x^*) = \frac{1 - x^*}{\tau_R}, \tag{4.17}$$

which may admit a nonzero solution (survival) or only $x^* = 0$ (collapse), depending on τ_R. A critical delay τ_R^c separates these regimes, analogous to a phase transition.

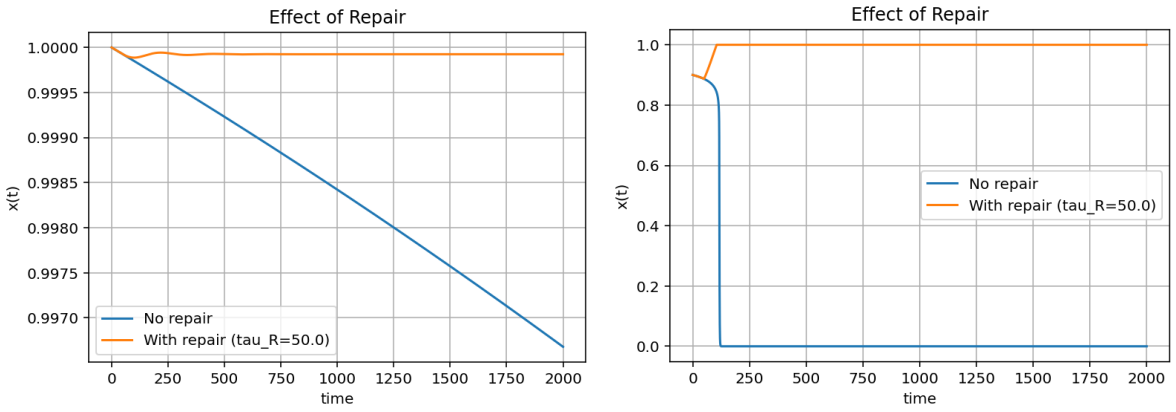


Figure 4.1: results of deterministic repair upon all-to-all network of size $N = 100$ and walkers $W = 2E$, with 4σ threshold. Two cases are shown: (left) When $x(t)$ is close to 1, and (right) when $x(t)$ has fallen below 0.9.

We crudely applied deterministic approximation to our network going through walker flux dynamics with repair. The dynamics reveal two distinct regimes. In the absence of repair, the system undergoes a rapid collapse driven by a positive feedback between load redistribution and node failures. This results in a finite-time transition to a completely inactive state.

In contrast, refer to the figure 4.1, the inclusion of a delayed repair mechanism stabilizes the system. For sufficiently small repair timescales, the system approaches a stable fixed point close to full activity. Near criticality, a balance between failure and repair leads to slow degradation or steady-state behavior. The delay in repair introduces memory effects, which can result in transient overshoots and small oscillations.

4.12 Recurrence Time and the Window for Repair

Figure 4.2 shows that as the network loses nodes, the recurrence time between successive extreme events decreases sharply. When it falls below unity, the network enters the cascade

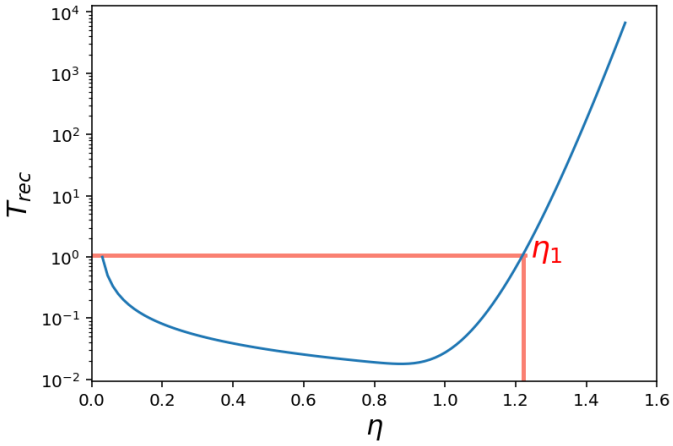


Figure 4.2: Recurrence time between extreme events as a function of the fraction of active nodes, for an all-to-all network ($N = 100$, threshold 4σ). The recurrence time drops below unity precisely at the transition from the independent to the cascade regime.

regime and experiences a rapid, irreversible collapse. Since the network spends $> 90\%$ of its lifetime in the *independent regime* (where extreme events are rare and spatially uncorrelated), this regime is the natural window for effective repair.

The comparison of repaired and unrepaired dynamics (figure 4.3 and 4.4) confirms that a finite repair delay $\tau_R = 50$ extends network lifetime without altering the qualitative trajectory through the η–F_{del} plane: a repaired and an unrepaired network are indistinguishable once the cascade begins. This leads to the concept of *slow repair* — repair initiated in the independent regime, where extreme events are infrequent and the resource demand is low.

4.13 Critical Repair Delay and the Survival Transition

Because extreme events are stochastic, the network failure time T_{fail} is a random variable. We define the failure probability

$$P_{\text{fail}}(\tau_R) = \frac{N_{\text{fail}}}{N_{\text{total}}}, \tag{4.18}$$

where N_{fail} is the number of realisations (in an ensemble of size N_{total}) that collapse before a fixed simulation time T_{sim}.

Figure 4.5 shows P_{fail} vs. τ_R for an all-to-all network ($N = 100$, $W = 2E$, threshold 4σ) at four simulation times. A clear transition region emerges: below the optimal delay τ_R^*

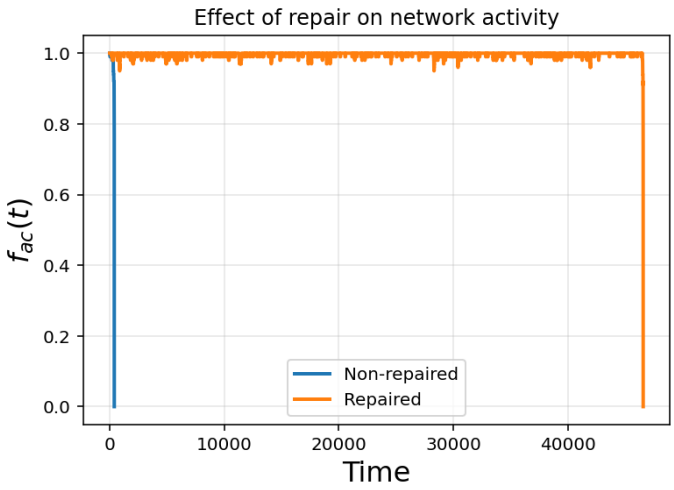


Figure 4.3: Fraction of active nodes vs. time for repaired ($\tau_R = 50$) and unrepaired networks ($N = 100$, $W = 9900$, threshold 4σ). Unrepaired network fails as usual following the network failure dynamics due to intrinsic fluctuations. Repair extends lifetime without changing the cascade dynamics.

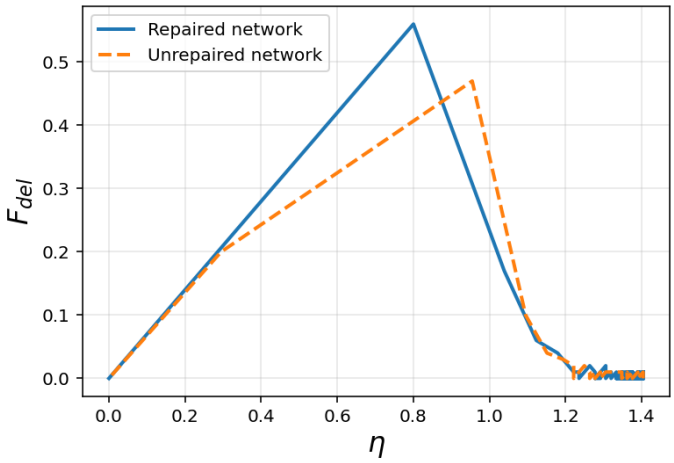


Figure 4.4: Load-to-capacity ratio η vs. fraction of deleted nodes F_{del} for repaired and unrepaired networks. The trajectories are identical once the cascade begins, confirming that repair opportunity lies exclusively in the independent regime.

the network survives, above it slow repair is no longer feasible. Crucially, a good estimate of τ_R^* is already obtained at modest simulation times ($\sim 10k$ steps), making the approach computationally tractable.

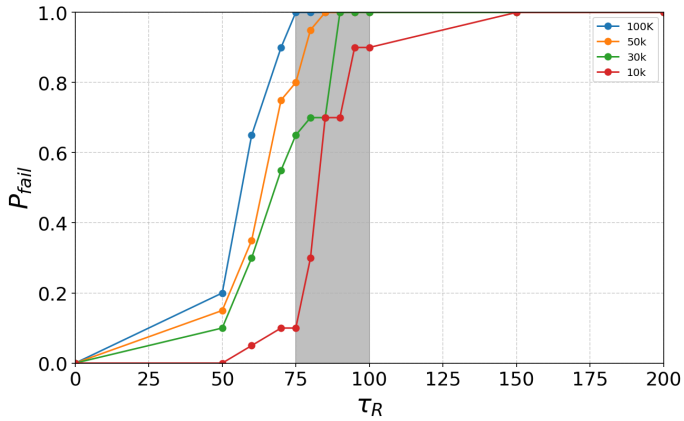


Figure 4.5: Failure probability P_{fail} as a function of repair delay τ_R for simulation times $10k, 30k, 50k, 100k$ (all-to-all, $N = 100$). The shaded region marks the transition beyond which slow repair fails.

A similar transition exists for scale-free networks (figure 4.6), though with a narrower transition window due to topological heterogeneity. As the threshold q increases, the independent regime widens, and τ_R^* grows correspondingly.

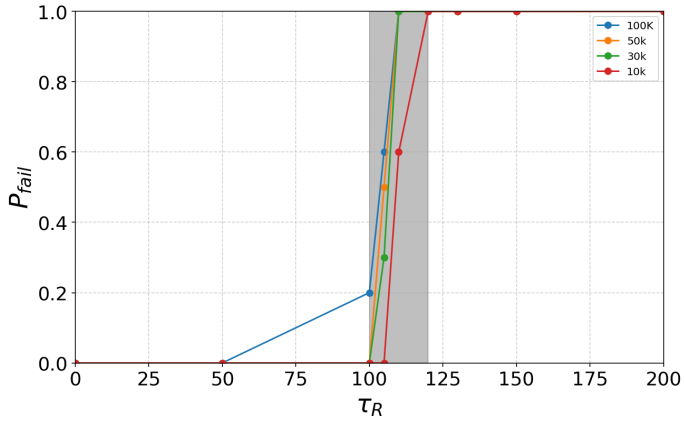


Figure 4.6: Failure probability P_{fail} vs. τ_R for a scale-free network ($N = 5000$, $W = 2E$, threshold 4σ, different coloured curves indicate simulation times $10k$–$100k$). The transition region is narrower than in the all-to-all case.

4.13.1 Regime-Dependent Repair: Slow vs Fast

The regime in which repair is initiated critically determines outcomes:

Independent regime (slow repair). Extreme events are isolated; repair with $\tau_R \lesssim \tau_R^*$ stabilises the network at low resource cost.

Cascade regime (fast repair). Near-instantaneous repair ($\tau_R \approx 1$) is required to return the network to the independent regime. The system oscillates between active and collapsed states, demanding sustained high effort.

Overload regime. Even $\tau_R = 1$ is insufficient. Walkers become trapped in isolated components; the network is effectively broken regardless of repair rate.

The comparison between fast repair cases in Cascade and Overload regimes are pointed in the f_{ac} vs t figure 4.7, where repair is attempted with $\tau_R = 1$ in both regimes, for a scale free network of $N = 5000$, with flux in 4σ threshold. Since this is a *fast repair* case, it is assumed that once the network exits the regimes, the repair dynamics is stopped due to the huge resource needed for the repair. Thus, we see an oscillatory motion when network exits cascade regime with fast repair, and then again enters after a while. This continues until the end of simulation time. Whereas in the repair in overload regime, since the nodes failing per time step is faster than repairs, the network's capacity-to-load ratio η becomes higher and exits the regime, stalling the fast-repairs. As we saw in the previous chapter, that isolated nodes' formation takes precedent during overload regimes, most of the walkers are stuck among the isolated nodes, which increases the η of the network. So, remaining few walkers in the network continue their dynamics in a broken network with almost no further extreme events. Thus, fast repair in the overload regime can save the structure of the network, but only by an imperfect load shedding.

This hierarchy underscores the importance of *early* intervention: once the cascade is established, the cost of repair grows dramatically, and recovery in the overload regime is essentially impossible under limited resources.

4.14 Structural Signatures of Failure

Given that early repair is optimal, we ask whether the network structure provides *advance warning* of impending failure. We rank nodes by their mean failure time computed over an

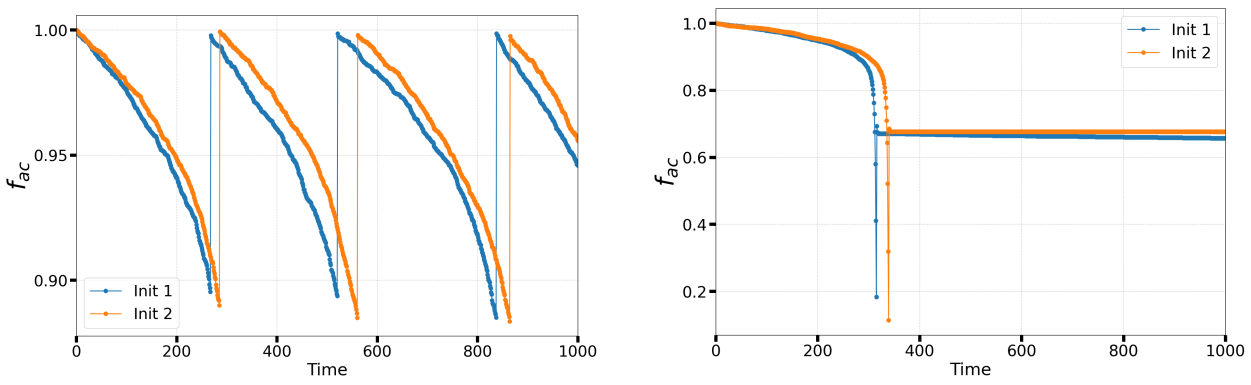


Figure 4.7: Comparison in cases for fast repair in scale free network: f_{ac} as a function of t for (left) Cascade regime and (right) Overload regime.

ensemble of at least ten independent realisations.

Networks studied: scale-free ($N = 500$, $E = 3936$, $W = 2E$) and Apollonian ($N = 500$, $E = 1494$, $W = 2E$).

The spring layout [120] positions strongly connected nodes closer together and weakly connected nodes farther apart, making it effective for identifying hubs, communities, and bridge nodes. Despite this, no definitive spatial pattern separates vulnerable from robust nodes by visual inspection alone (figure 4.8).

Figure 4.9 reveals a clear degree-based signature: *low-degree nodes fail first*, but they do so individually rather than as a coherent group. The cascade is triggered when nodes of intermediate degree ($\langle k \rangle \approx 40$–$70$ in both networks) begin to fail. Thus, the onset of intermediate-degree node failure is a reliable early warning indicator.

Comparing the top-10 most vulnerable and most robust nodes (figure 4.10), robust nodes consistently exhibit higher degree — both initially and at the point of deletion. Their k-core values and mean neighbour degrees decline over time as surrounding low-degree nodes are removed, but they outlast the rest of the network precisely because of their structural centrality, which can be compared by forming the first hop neighbour subgraph of the vulnerable and robust nodes. The density of the subgraphs formed, $\rho_{robust} \approx 2\rho_{vulnerable}$. This was evident in both the networks used.

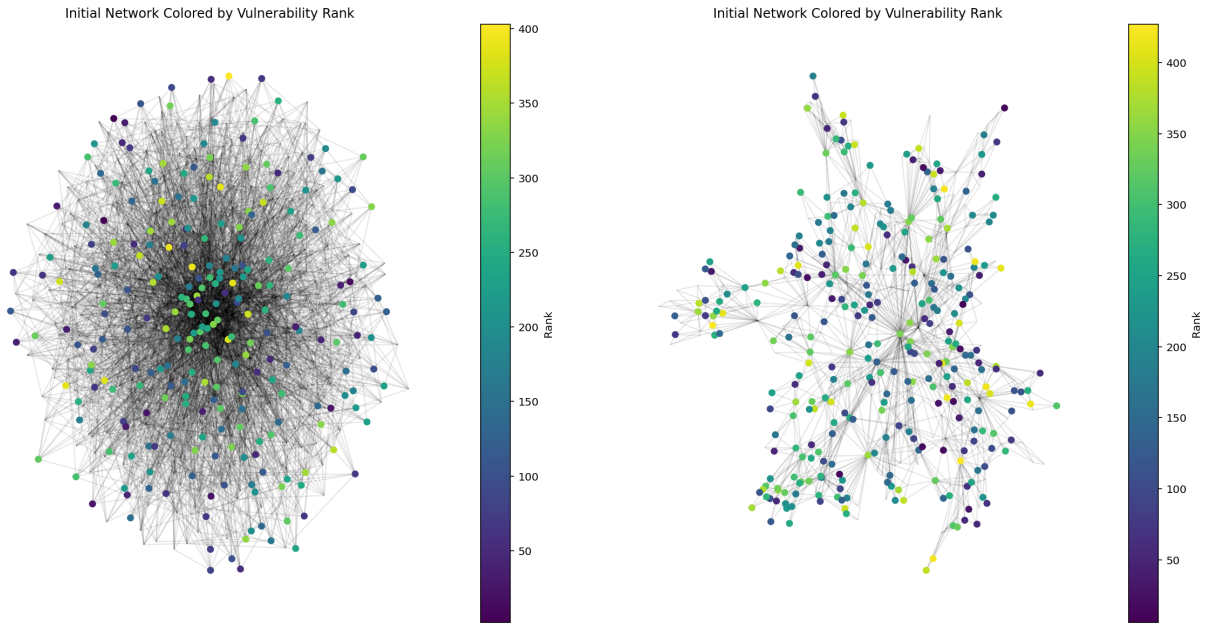


Figure 4.8: Networks visualised (Fruchterman–Reingold spring layout, NetworkX) with nodes coloured by vulnerability rank. Left: scale-free; Right: Apollonian. Dark blue implies more vulnerability whereas yellow does robustness.

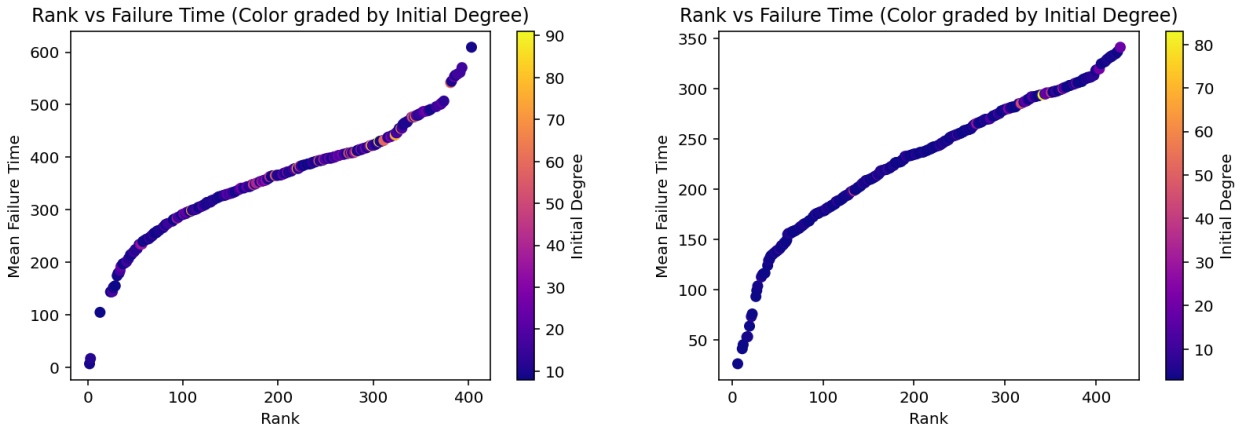


Figure 4.9: Rank vs. mean failure time, colour-coded by initial degree. Left: scale-free; Right: Apollonian. Low-degree nodes fail first; the network enters the cascade regime when intermediate-degree nodes begin to fail.

4.15 Summary

This chapter has developed a unified view of repair in complex networks: Repair spans structural and functional dimensions, operates across a spectrum of timescales, and can be

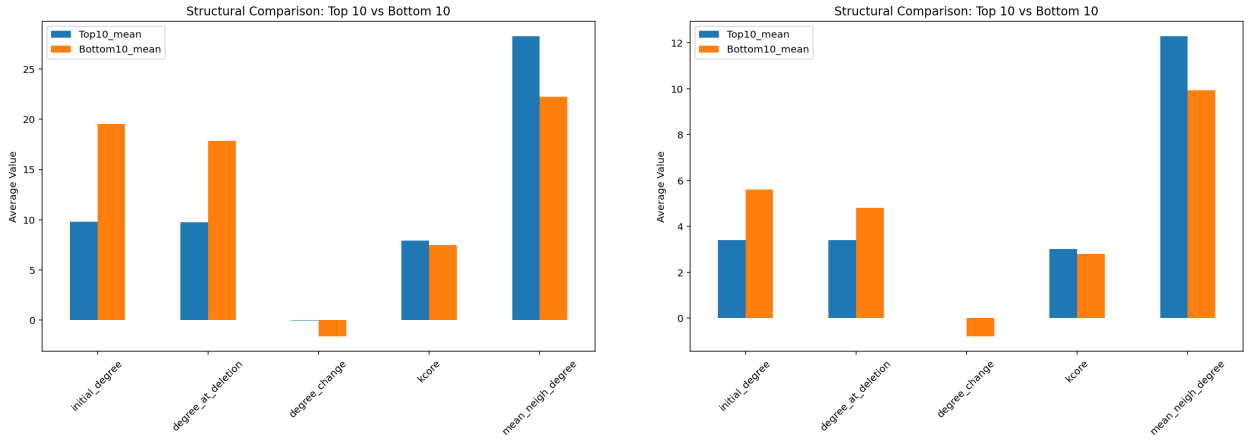


Figure 4.10: Structural comparison of the 10 most vulnerable and 10 most robust nodes: initial degree, degree at deletion, degree change, k-core, and mean neighbour degree. Left: scale-free; Right: Apollonian.

local (rewiring, self-healing) or global (optimization, centralized control). Network topology — especially hub structure and clustering — profoundly affects repair efficiency. Starting from a random-walk flux model, we derived a nonlinear DDE (eq. (4.16)) that captures the competition between state-dependent failure and delayed recovery. A critical repair delay τ_R^c separates survival from collapse, analogous to a phase transition.

Slow repair in the independent regime is both effective and resource-efficient. Once the cascade or overload regime is entered, repair demands escalate sharply and eventually become infeasible. The repaired and non-repaired networks follow the same three regime failure. So, effectively the network dynamics remains unchanged in the slow repair states. Fast repairs result in imperfect load shedding.

The sequential failure of low-degree nodes, culminating in the failure of intermediate-degree nodes, provides a structural early-warning signal. Monitoring this transition can guide targeted preemptive repair.

Together, these results provide a quantitative framework for designing repair strategies in networks subjected to intrinsic stochastic fluctuations, with direct implications for infrastructure resilience, biological network maintenance, and the engineering of robust distributed systems.

Chapter 5

Conclusion

5.1 Summary of Results

This thesis has investigated how large-scale network failure can emerge purely from intrinsic stochastic fluctuations in node flux, without any external attack or perturbation. Using multiple random walkers as a model for flux transport, extreme events were defined as instances where the instantaneous walker count at a node exceeded a degree-dependent threshold, and the consequences of such events were traced from isolated nodal failures through to complete network collapse.

The central finding is that network failure induced by intrinsic fluctuations is not an abrupt, unpredictable event but a *structured process* that unfolds through three universally observable regimes. In the *independent failure* regime, extreme events are rare and spatially uncorrelated; the network sustains near-normal operation and the capacity-to-load ratio η remains well above unity. As η decreases, the system crosses into the *cascade failure* regime, where individual node failures redistribute load onto neighbours, triggering correlated bursts of secondary failures. Finally, the *overload* regime marks the terminal phase, in which the residual capacity falls so far below the total load that all remaining nodes fail within one or two time steps. This three-regime structure was demonstrated analytically for the all-to-all network and confirmed numerically across Erdős–Rényi, Barabási–Albert, Watts–Strogatz, square-lattice, and real-world flight and road networks, establishing its universality.

Chapter 4 extended this picture by introducing delayed repair dynamics. A nonlinear delay

differential equation captures the competition between state-dependent failure and recovery, and predicts a critical repair delay τ_R^* that separates a survival phase from irreversible collapse – a phase transition analogous to percolation thresholds in classical network robustness theory. The key practical insight is that *slow repair* initiated during the independent regime is both sufficient and resource-efficient; once the cascade is established, repair demands escalate sharply and recovery becomes effectively impossible in the overload regime. Analysis of failure-time rankings across scale-free and Apollonian networks further revealed that low-degree nodes fail first, but the cascade is triggered by the onset of intermediate-degree node failure, providing a structural early-warning indicator that is observable in real time.

The results challenge a prevailing assumption in infrastructure resilience: that robustness requires only protection against external shocks. The analyses presented here demonstrate that internal fluctuations – ubiquitous in power grids, road networks, and communication systems – are themselves sufficient to drive progressive, irreversible collapse. The capacity-to-load ratio η emerges as a unifying order parameter that collapses realizations from different initial conditions onto a single universal curve, making it a practical diagnostic for real-time monitoring of network health.

5.2 Limitations and Future Directions

Several simplifying assumptions open avenues for future work. Throughout this thesis, failed nodes were assumed to fail permanently unless explicitly repaired; relaxing this to incorporate stochastic, heterogeneous repair times would bring the model closer to realistic infrastructure scenarios. The random-walker flux model, while analytically tractable, does not capture directed or capacity-constrained flow; extending the framework to flow networks governed by Kirchhoff's laws or queueing-theoretic dynamics would broaden applicability to power grids and communication networks directly.

The present work has focused on intrinsic fluctuation-induced failures in undirected and unweighted networks with transport modeled through random walkers. Several promising directions remain for future investigation. One natural extension is to study failure and recovery processes in directed and weighted networks, where heterogeneous interactions and asymmetric transport may significantly influence the onset and propagation of cascading failures. Another important direction is to couple the failure mechanism with dynamical processes occurring on the nodes themselves, such as synchronization, epidemic spreading,

neuronal activity, or oscillator dynamics. Investigating the interplay between network topology, transport dynamics, and node dynamics may provide a more comprehensive understanding of failure mechanisms in complex systems and lead to more effective intervention and recovery strategies in realistic networks.

Furthermore, the present study focused on single-layer networks. Many real infrastructures are interdependent – power grids rely on communication networks, which in turn depend on the power grid – and intrinsic fluctuations in one layer may nucleate cascades in another. Extending the three-regime framework to multiplex and interdependent networks is a natural and pressing direction. Finally, the early-warning signatures identified here – recurrence-time collapse and intermediate-degree node failure – could be embedded into data-driven monitoring frameworks, combining the analytical results of this thesis with graph neural networks or changepoint-detection algorithms to yield practical, real-time alert systems for large-scale networked infrastructures.

Bibliography

[1] Reuven Cohen and Shlomo Havlin. *Complex Networks: Structure, Robustness and Function*. Cambridge: Cambridge University Press, 2010.

[2] Albert-László Barabási. *Network Science*. Also available at http://networksciencebook.com. Cambridge: Cambridge University Press, 2016.

[3] *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. https://www.energy.gov/oe/articles/blackout-2003-final-report-august-14-2003-blackout-united-states-and-canada-causes-and. U.S. Department of Energy. Accessed: 18 February 2024.

[4] Central Electricity Authority. *Report on the Grid Disturbances on 30th July 2012 and 31st July 2012*. Submitted in compliance with CERC Order (Petition No. 167/Suo-Motu/2012). Ministry of Power, Government of India, Aug. 2012.

[5] Réka Albert, Hawoong Jeong, and Albert-László Barabási. "Error and attack tolerance of complex networks". In: *Nature* 406.6794 (2000), pp. 378–382. DOI: 10.1038/35019019.

[6] Reuven Cohen et al. "Breakdown of the Internet under Intentional Attack". In: *Phys. Rev. Lett.* 86 (16 Apr. 2001), pp. 3682–3685. DOI: 10.1103/PhysRevLett.86.3682. URL: https://link.aps.org/doi/10.1103/PhysRevLett.86.3682.

[7] Ying-Cheng Lai, Adilson E. Motter, and Takashi Nishikawa. "Attacks and cascades in complex networks". In: *Lecture Notes in Physics* 650 (2004), pp. 299–310.

[8] Vimal Kishore, M. S. Santhanam, and R. E. Amritkar. "Extreme Events on Complex Networks". In: *Phys. Rev. Lett.* 106 (18 May 2011), p. 188701. DOI: 10.1103/PhysRevLett.106.188701. URL: https://link.aps.org/doi/10.1103/PhysRevLett.106.188701.

[9] Sayantan Nag Chowdhury et al. "Extreme events in dynamical systems and random walkers: A review". In: *Physics Reports* 966 (2022). Extreme events in dynamical

systems and random walkers: A review, pp. 1–52. ISSN: 0370-1573. DOI: https://doi.org/10.1016/j.physrep.2022.04.001. URL: https://www.sciencedirect.com/science/article/pii/S0370157322001144.

[10] Govind Gandhi and M. S. Santhanam. "Biased random walkers and extreme events on the edges of complex networks". In: *Phys. Rev. E* 105 (1 Jan. 2022), p. 014315. DOI: 10.1103/PhysRevE.105.014315. URL: https://link.aps.org/doi/10.1103/PhysRevE.105.014315.

[11] Vimal Kishore, M. S. Santhanam, and R. E. Amritkar. "Extreme events and event size fluctuations in biased random walks on networks". In: *Phys. Rev. E* 85 (5 May 2012), p. 056120. DOI: 10.1103/PhysRevE.85.056120. URL: https://link.aps.org/doi/10.1103/PhysRevE.85.056120.

[12] Adilson E. Motter and Ying-Cheng Lai. "Cascade-based attacks on complex networks". In: *Phys. Rev. E* 66 (6 Dec. 2002), p. 065102. DOI: 10.1103/PhysRevE.66.065102. URL: https://link.aps.org/doi/10.1103/PhysRevE.66.065102.

[13] Lucas D Valdez et al. "Cascading failures in complex networks". In: *Journal of Complex Networks* 8.2 (May 2020), cnaa013. ISSN: 2051-1329. DOI: 10.1093/comnet/cnaa013. eprint: https://academic.oup.com/comnet/article-pdf/8/2/cnaa013/33582729/cnaa013.pdf. URL: https://doi.org/10.1093/comnet/cnaa013.

[14] Xueming Liu et al. "Network resilience". In: *Physics Reports* 971 (2022). Network Resilience, pp. 1–108. ISSN: 0370-1573. DOI: https://doi.org/10.1016/j.physrep.2022.04.002. URL: https://www.sciencedirect.com/science/article/pii/S0370157322001211.

[15] Thilo Gross and Laura Barth. "Network Robustness Revisited". In: *Frontiers in Physics* 10 (2022). ISSN: 2296-424X. DOI: 10.3389/fphy.2022.823564. URL: https://www.frontiersin.org/articles/10.3389/fphy.2022.823564.

[16] Marcus Engsig, Alejandro Tejedor, and Yamir Moreno. "Robustness assessment of complex networks using the idle network". In: *Phys. Rev. Res.* 4 (4 Dec. 2022), p. L042050. DOI: 10.1103/PhysRevResearch.4.L042050. URL: https://link.aps.org/doi/10.1103/PhysRevResearch.4.L042050.

[17] Yang Yang, Takashi Nishikawa, and Adilson E. Motter. "Small vulnerable sets determine large network cascades in power grids". In: *Science* 358.6365 (2017), eaan3184. DOI: 10.1126/science.aan3184.

[18] Marten Scheffer et al. "Early-warning signals for critical transitions". In: *Nature* 461.7260 (2009), pp. 53–59. DOI: 10.1038/nature08227.

[19] Ginestra Bianconi et al. "Complex systems in the spotlight: next steps after the 2021 Nobel Prize in Physics". In: *Journal of Physics: Complexity* 4.1 (Jan. 2023), p. 010201. DOI: 10.1088/2632-072X/ac7f75. URL: https://dx.doi.org/10.1088/2632-072X/ac7f75.

[20] Emil Julius Gumbel. *Statistics of Extremes*. New York: Columbia University Press, 1958.

[21] Kritika Gupta and M. S. Santhanam. "Extreme events in Nagel–Schreckenberg model of traffic flow on complex networks". In: *The European Physical Journal Special Topics* 230 (2021), pp. 3201–3209. DOI: 10.1140/epjs/s11734-021-00171-4.

[22] Mark E. J. Newman. *Networks: An Introduction*. Oxford: Oxford University Press, 2010. ISBN: 978-0-19-920665-0.

[23] Steven H. Strogatz. "Exploring complex networks". In: *Nature* 410.6825 (2001), pp. 268–276. DOI: 10.1038/35065725.

[24] Giuliano Andrea Pagani and Marco Aiello. "The Power Grid as a complex network: A survey". In: *Physica A: Statistical Mechanics and its Applications* 392.11 (2013), pp. 2688–2700. ISSN: 0378-4371. DOI: https://doi.org/10.1016/j.physa.2013.01.023. URL: https://www.sciencedirect.com/science/article/pii/S0378437113000575.

[25] Dirk Witthaut et al. "Collective nonlinear dynamics and self-organization in decentralized power grids". In: *Rev. Mod. Phys.* 94 (1 Feb. 2022), p. 015005. DOI: 10.1103/RevModPhys.94.015005. URL: https://link.aps.org/doi/10.1103/RevModPhys.94.015005.

[26] Paul Erdős and Alfréd Rényi. "On Random Graphs I". In: *Publicationes Mathematicae Debrecen* 6 (1959), pp. 290–297.

[27] Paul Erdős and Alfréd Rényi. "On the Evolution of Random Graphs". In: *Publications of the Mathematical Institute of the Hungarian Academy of Sciences* 5 (1960), pp. 17–61.

[28] Duncan J. Watts and Steven H. Strogatz. "Collective dynamics of 'small-world' networks". In: *Nature* 393.6684 (1998), pp. 440–442. DOI: 10.1038/30918.

[29] Albert-László Barabási and Réka Albert. "Emergence of Scaling in Random Networks". In: *Science* 286.5439 (1999), pp. 509–512. DOI: 10.1126/science.286.5439.509.

[30] Romualdo Pastor-Satorras and Alessandro Vespignani. "Epidemic Spreading in Scale-Free Networks". In: *Phys. Rev. Lett.* 86 (Apr. 2001), pp. 3200–3203. DOI: 10.1103/PhysRevLett.86.3200.

[31] Reuven Cohen and Shlomo Havlin. "Scale-Free Networks Are Ultrasmall". In: *Phys. Rev. Lett.* 90 (Feb. 2003), p. 058701. DOI: 10.1103/PhysRevLett.90.058701.

[32] Stefano Boccaletti et al. "Complex networks: Structure and dynamics". In: *Physics Reports* 424.4–5 (2006), pp. 175–308. DOI: 10.1016/j.physrep.2005.10.009.

[33] Linton C. Freeman. "A set of measures of centrality based on betweenness". In: *Sociometry* 40.1 (1977), pp. 35–41. DOI: 10.2307/3033543.

[34] Phillip Bonacich. "Power and centrality: A family of measures". In: *American Journal of Sociology* 92.5 (1987), pp. 1170–1182. DOI: 10.1086/228631.

[35] Michelle Girvan and Mark E. J. Newman. "Community structure in social and biological networks". In: *Proceedings of the National Academy of Sciences* 99.12 (2002), pp. 7821–7826. DOI: 10.1073/pnas.122653799.

[36] Mark E. J. Newman and Michelle Girvan. "Finding and evaluating community structure in networks". In: *Phys. Rev. E* 69 (Feb. 2004), p. 026113. DOI: 10.1103/PhysRevE.69.026113.

[37] Paul L. Krapivsky, Sidney Redner, and Francois Leyvraz. "Connectivity of Growing Random Networks". In: *Phys. Rev. Lett.* 85 (Nov. 2000), pp. 4629–4632. DOI: 10.1103/PhysRevLett.85.4629.

[38] Konstantin Klemm and Víctor M. Eguíluz. "Highly clustered scale-free networks". In: *Phys. Rev. E* 65 (Mar. 2002), p. 036123. DOI: 10.1103/PhysRevE.65.036123.

[39] Ginestra Bianconi and Albert-László Barabási. "Competition and multiscaling in evolving networks". In: *Europhysics Letters* 54.4 (2001), pp. 436–442. DOI: 10.1209/epl/i2001-00260-6.

[40] Louis M. Pecora and Thomas L. Carroll. "Master Stability Functions for Synchronized Coupled Systems". In: *Phys. Rev. Lett.* 80 (Mar. 1998), pp. 2109–2112. DOI: 10.1103/PhysRevLett.80.2109.

[41] Jae Dong Noh and Heiko Rieger. "Random Walks on Complex Networks". In: *Phys. Rev. Lett.* 92 (11 Mar. 2004), p. 118701. DOI: 10.1103/PhysRevLett.92.118701. URL: https://link.aps.org/doi/10.1103/PhysRevLett.92.118701.

[42] Paolo Crucitti, Vito Latora, and Massimo Marchiori. "Model for cascading failures in complex networks". In: *Phys. Rev. E* 69 (4 Apr. 2004), p. 045104. DOI: 10.1103/

PhysRevE.69.045104. URL: https://link.aps.org/doi/10.1103/PhysRevE.69.045104.

[43] Vedang Tamhane and G Ambika. "Structure and stability of the Indian power transmission network". In: *Journal of Physics: Complexity* 4.2 (May 2023), p. 025014. DOI: 10.1088/2632-072X/acd611. URL: https://dx.doi.org/10.1088/2632-072X/acd611.

[44] Alain Barrat, Marc Barthélemy, and Alessandro Vespignani. *Dynamical Processes on Complex Networks*. Cambridge: Cambridge University Press, 2008. ISBN: 978-0-521-87950-7.

[45] Romualdo Pastor-Satorras and Alessandro Vespignani. "Epidemic dynamics and endemic states in complex networks". In: *Physical Review E* 63.6 (2001), p. 066117. DOI: 10.1103/PhysRevE.63.066117.

[46] Florian Dörfler and Francesco Bullo. "Synchronization in complex networks of phase oscillators: A survey". In: *Automatica* 50.6 (2014), pp. 1539–1564. DOI: 10.1016/j.automatica.2014.04.012.

[47] Michalis Faloutsos, Petros Faloutsos, and Christos Faloutsos. "On power-law relationships of the internet topology". In: *ACM SIGCOMM Computer Communication Review* 29.4 (1999), pp. 251–262. DOI: 10.1145/316194.316229.

[48] Sergey V. Buldyrev et al. "Catastrophic cascade of failures in interdependent networks". In: *Nature* 464 (2010), pp. 1025–1028. DOI: 10.1038/nature08932.

[49] D. J. Watts. "A simple model of global cascades on random networks". In: *Proceedings of the National Academy of Sciences* 99.9 (2002), pp. 5766–5771. DOI: 10.1073/pnas.082090499.

[50] Réka Albert and Albert-László Barabási. "Statistical mechanics of complex networks". In: *Reviews of Modern Physics* 74.1 (2002), pp. 47–97. DOI: 10.1103/RevModPhys.74.47.

[51] Alex Arenas et al. "Synchronization in complex networks". In: *Physics Reports* 469.3 (2008), pp. 93–153. DOI: 10.1016/j.physrep.2008.09.002.

[52] Thilo Gross and Bernd Blasius. "Adaptive coevolutionary networks: a review". In: *Journal of the Royal Society Interface* 5.20 (2008), pp. 259–271. DOI: 10.1098/rsif.2007.1229.

[53] Dimitris Achlioptas, Raissa M. D'Souza, and Joel Spencer. "Explosive Percolation in Random Networks". In: *Science* 323.5920 (2009), pp. 1453–1455. DOI: 10.1126/science.1167782.

[54] Duncan S. Callaway et al. “Network Robustness and Fragility: Percolation on Random Graphs”. In: *Physical Review Letters* 85.25 (2000), pp. 5468–5471. DOI: 10.1103/PhysRevLett.85.5468.

[55] Béla Bollobás. *Random Graphs*. 2nd. Cambridge: Cambridge University Press, 2001. ISBN: 978-0-521-79722-1.

[56] M. E. J. Newman, S. H. Strogatz, and D. J. Watts. “Random graphs with arbitrary degree distributions and their applications”. In: *Physical Review E* 64.2 (2001), p. 026118. DOI: 10.1103/PhysRevE.64.026118.

[57] Alexei Vázquez and Yamir Moreno. “Resilience to damage of graphs with degree correlations”. In: *Physical Review E* 67.1 (2003), 015101(R). DOI: 10.1103/PhysRevE.67.015101.

[58] Romualdo Pastor-Satorras et al. “Epidemic processes in complex networks”. In: *Reviews of Modern Physics* 87.3 (2015), pp. 925–979. DOI: 10.1103/RevModPhys.87.925.

[59] Matt J. Keeling and Pejman Rohani. *Modeling Infectious Diseases in Humans and Animals*. Princeton: Princeton University Press, 2008. ISBN: 978-0-691-11617-4.

[60] Yang Wang et al. “Epidemic spreading in real networks: An eigenvalue viewpoint”. In: (2003), pp. 25–34. DOI: 10.1109/RELDIS.2003.1238052.

[61] Deepayan Chakrabarti et al. “Epidemic Thresholds in Real Networks”. In: *ACM Transactions on Information and System Security* 10.4 (2008), pp. 1–26. DOI: 10.1145/1284680.1284681.

[62] Peter Grassberger. “On the critical behavior of the general epidemic process and dynamical percolation”. In: *Mathematical Biosciences* 63.2 (1983), pp. 157–172. DOI: 10.1016/0025-5564(83)90028-4.

[63] M. E. J. Newman. “Spread of epidemic disease on networks”. In: *Physical Review E* 66.1 (2002), p. 016128. DOI: 10.1103/PhysRevE.66.016128.

[64] Andrey Y. Lokhov et al. “Inferring the origin of an epidemic with a dynamic message-passing algorithm”. In: *Physical Review E* 90.1 (2014), p. 012801. DOI: 10.1103/PhysRevE.90.012801.

[65] Steven H. Strogatz. *Sync: The Emerging Science of Spontaneous Order*. New York: Hyperion, 2003. ISBN: 978-0-7868-8721-7.

[66] Yoshiki Kuramoto. *Chemical Oscillations, Waves, and Turbulence*. Springer Series in Synergetics. Berlin: Springer, 1984. DOI: 10.1007/978-3-642-69689-3.

[67] Juan A. Acebrón et al. “The Kuramoto model: A simple paradigm for synchronization phenomena”. In: *Reviews of Modern Physics* 77.1 (2005), pp. 137–185. DOI: 10.1103/RevModPhys.77.137.

[68] Jesús Gómez-Gardeñes et al. “Explosive Synchronization Transitions in Scale-Free Networks”. In: *Physical Review Letters* 106.12 (2011), p. 128701. DOI: 10.1103/PhysRevLett.106.128701.

[69] Alex Arenas, Albert Díaz-Guilera, and Conrad J. Pérez-Vicente. “Synchronization Reveals Topological Scales in Complex Networks”. In: *Physical Review Letters* 96.11 (2006), p. 114102. DOI: 10.1103/PhysRevLett.96.114102.

[70] Mauricio Barahona and Louis M. Pecora. “Synchronization in Small-World Systems”. In: *Physical Review Letters* 89.5 (2002), p. 054101. DOI: 10.1103/PhysRevLett.89.054101.

[71] Claudio Castellano, Santo Fortunato, and Vittorio Loreto. “Statistical physics of social dynamics”. In: *Reviews of Modern Physics* 81.2 (2009), pp. 591–646. DOI: 10.1103/RevModPhys.81.591.

[72] Vishal Sood and Sidney Redner. “Voter Model on Heterogeneous Graphs”. In: *Physical Review Letters* 94.17 (2005), p. 178701. DOI: 10.1103/PhysRevLett.94.178701.

[73] Vishal Sood, Tibor Antal, and Sidney Redner. “Voter models on heterogeneous graphs”. In: *Physical Review E* 77.4 (2008), p. 041121. DOI: 10.1103/PhysRevE.77.041121.

[74] J. Theodore Cox. “Coalescing Random Walks and Voter Model Consensus Times on the Torus in $\mathbb{Z}^d$”. In: *The Annals of Probability* 17.4 (1989), pp. 1333–1366. DOI: 10.1214/aop/1176991158.

[75] Mark Granovetter. “Threshold Models of Collective Behavior”. In: *American Journal of Sociology* 83.6 (1978), pp. 1420–1443. DOI: 10.1086/226707.

[76] Prasanna Gai and Sujit Kapadia. “Contagion in financial networks”. In: *Proceedings of the Royal Society A* 466.2120 (2010), pp. 2401–2423. DOI: 10.1098/rspa.2009.0410.

[77] Martin A. Nowak. *Evolutionary Dynamics: Exploring the Equations of Life*. Cambridge, MA: Harvard University Press, 2006. ISBN: 978-0-674-02338-3.

[78] Martin A. Nowak and Robert M. May. “Evolutionary games and spatial chaos”. In: *Nature* 359 (1992), pp. 826–829. DOI: 10.1038/359826a0.

[79] Francisco C. Santos and Jorge M. Pacheco. “Scale-free networks provide a unifying framework for the emergence of cooperation”. In: *Physical Review Letters* 95.9 (2005), p. 098104. DOI: 10.1103/PhysRevLett.95.098104.

[80] László Lovász. "Random Walks on Graphs: A Survey". In: *Bolyai Society Mathematical Studies* 2 (1993), pp. 1–46.

[81] Sameet Sreenivasan et al. "Structural bottlenecks for communication in networks". In: *Physical Review E* 75.3 (2007), p. 036105. DOI: 10.1103/PhysRevE.75.036105.

[82] Arda Halu et al. "Multiplex PageRank". In: *PLOS ONE* 8.10 (2013), e78293. DOI: 10.1371/journal.pone.0078293.

[83] Paul Embrechts, Claudia Klüppelberg, and Thomas Mikosch. *Modelling Extremal Events for Insurance and Finance*. Applications of Mathematics. Berlin: Springer, 1997. DOI: 10.1007/978-3-642-33483-2.

[84] Richard W. Katz, Grace S. Brush, and Marc B. Parlange. "Statistics of extremes: Modeling ecological disturbances". In: *Ecology* 86.5 (2005), pp. 1124–1134. DOI: 10.1890/04-0606.

[85] Ronald A. Fisher and Leonard H. C. Tippett. "Limiting forms of the frequency distribution of the largest or smallest member of a sample". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 24.2 (1928), pp. 180–190. DOI: 10.1017/S0305004100015681.

[86] Boris Vladimirovich Gnedenko. "Sur la distribution limite du terme maximum d'une série aléatoire". In: *Annals of Mathematics* 44.3 (1943), pp. 423–453. DOI: 10.2307/1968974.

[87] Stuart Coles. *An Introduction to Statistical Modeling of Extreme Values*. Springer Series in Statistics. London: Springer, 2001. DOI: 10.1007/978-1-4471-3675-0.

[88] Arthur F. Jenkinson. "The frequency distribution of the annual maximum (or minimum) values of meteorological elements". In: *Quarterly Journal of the Royal Meteorological Society* 81.348 (1955), pp. 158–171. DOI: 10.1002/qj.49708134804.

[89] James Pickands. "Statistical Inference Using Extreme Order Statistics". In: *The Annals of Statistics* 3.1 (1975), pp. 119–131. DOI: 10.1214/aos/1176343003.

[90] Anthony C. Davison and Richard L. Smith. "Models for Exceedances over High Thresholds". In: *Journal of the Royal Statistical Society: Series B* 52.3 (1990), pp. 393–425. DOI: 10.1111/j.2517-6161.1990.tb01796.x.

[91] August A. Balkema and Laurens de Haan. "Residual Life Time at Great Age". In: *The Annals of Probability* 2.5 (1974), pp. 792–804. DOI: 10.1214/aop/1176996548.

[92] Armin Bunde et al. "Long-Term Memory: A Natural Mechanism for the Clustering of Extreme Events and Anomalous Residual Times in Climate Records". In: *Physical Review Letters* 94.4 (2005), p. 048701. DOI: 10.1103/PhysRevLett.94.048701.

[93] Malcolm R. Leadbetter, Georg Lindgren, and Holger Rootzén. *Extremes and Related Properties of Random Sequences and Processes*. Springer Series in Statistics. New York: Springer, 1983. DOI: 10.1007/978-1-4612-5449-2.

[94] Sidney I. Resnick. *Extreme Values, Regular Variation and Point Processes*. Applied Probability. New York: Springer, 1987. DOI: 10.1007/978-0-387-75953-1.

[95] Ian Dobson et al. "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization". In: *Chaos* 17.2 (2007), p. 026103. DOI: 10.1063/1.2737822.

[96] Alan G. Hawkes. "Spectra of Some Self-Exciting and Mutually Exciting Point Processes". In: *Biometrika* 58.1 (1971), pp. 83–90. DOI: 10.1093/biomet/58.1.83.

[97] Jonathan R. M. Hosking. "L-Moments: Analysis and Estimation of Distributions Using Linear Combinations of Order Statistics". In: *Journal of the Royal Statistical Society: Series B* 52.1 (1990), pp. 105–124. DOI: 10.1111/j.2517-6161.1990.tb01775.x.

[98] Alec G. Stephenson and Jonathan A. Tawn. "Bayesian inference for extremes: accounting for the three extremal types". In: *Extremes* 7.4 (2004), pp. 291–307. DOI: 10.1007/s10687-004-3479-6.

[99] Réka Albert, István Albert, and Gary L. Nakarado. "Structural vulnerability of the North American power grid". In: *Phys. Rev. E* 69 (2 Feb. 2004), p. 025103. DOI: 10.1103/PhysRevE.69.025103. URL: https://link.aps.org/doi/10.1103/PhysRevE.69.025103.

[100] Franz Kaiser, Vito Latora, and Dirk Witthaut. "Network isolators inhibit failure spreading in complex networks". In: *Nature Communications* 12 (2021), p. 3143. DOI: 10.1038/s41467-021-23292-9.

[101] Asim K. Dey, Yulia R. Gel, and H. Vincent Poor. "What network motifs tell us about resilience and reliability of complex networks". In: *Proceedings of the National Academy of Sciences* 116.39 (2019), pp. 19368–19373. DOI: 10.1073/pnas.1819529116. eprint: https://www.pnas.org/doi/pdf/10.1073/pnas.1819529116. URL: https://www.pnas.org/doi/abs/10.1073/pnas.1819529116.

[102] J Heitzig et al. *Interdisciplinary challenges in the study of power grid resilience and stability and their relation to extreme weather events*. 2014.

[103] Jussara Dias, Arthur N. Montanari, and Elbert E. N. Macau. "Power-grid vulnerability and its relation with network structure". In: *Chaos: An Interdisciplinary Journal of Nonlinear Science* 33.3 (Mar. 2023), p. 033122. ISSN: 1054-1500. DOI: 10.1063/5.0137919. eprint: https://pubs.aip.org/aip/cha/article-pdf/

doi/10.1063/5.0137919/16789015/033122_1_online.pdf. URL: https://doi.org/10.1063/5.0137919.

[104] John C. Doyle et al. "The "robust yet fragile" nature of the Internet". In: *Proceedings of the National Academy of Sciences* 102.41 (2005), pp. 14497–14502. DOI: 10.1073/pnas.0501426102. eprint: https://www.pnas.org/doi/pdf/10.1073/pnas.0501426102. URL: https://www.pnas.org/doi/abs/10.1073/pnas.0501426102.

[105] Yosef Kornbluth et al. "Network overload due to massive attacks". In: *Phys. Rev. E* 97 (5 May 2018), p. 052309. DOI: 10.1103/PhysRevE.97.052309. URL: https://link.aps.org/doi/10.1103/PhysRevE.97.052309.

[106] Benjamin A Carreras et al. "Complex dynamics of blackouts in power transmission systems". In: *Chaos: An Interdisciplinary Journal of Nonlinear Science* 14.3 (2004), pp. 643–652.

[107] Rezoan Ahmed Shuvro et al. "Data-Integrity Aware Stochastic Model for Cascading Failures in Power Grids". In: *IEEE Transactions on Power Systems* 38.1 (2023), pp. 142–154. DOI: 10.1109/TPWRS.2022.3164671.

[108] Tommaso Nesti, Fiona Sloothaak, and Bert Zwart. "Emergence of Scale-Free Blackout Sizes in Power Grids". In: *Phys. Rev. Lett.* 125 (5 July 2020), p. 058301. DOI: 10.1103/PhysRevLett.125.058301. URL: https://link.aps.org/doi/10.1103/PhysRevLett.125.058301.

[109] Jung-Hoon Jung and Young-Ho Eom. "Empirical analysis of congestion spreading in Seoul traffic network". In: *Phys. Rev. E* 108 (5 Nov. 2023), p. 054312. DOI: 10.1103/PhysRevE.108.054312. URL: https://link.aps.org/doi/10.1103/PhysRevE.108.054312.

[110] Zhuoran Chen et al. "Recursive traffic percolation on urban transportation systems". In: *Chaos: An Interdisciplinary Journal of Nonlinear Science* 33.3 (Mar. 2023), p. 033132. ISSN: 1054-1500. DOI: 10.1063/5.0137726. eprint: https://pubs.aip.org/aip/cha/article-pdf/doi/10.1063/5.0137726/16789779/033132_1_online.pdf. URL: https://doi.org/10.1063/5.0137726.

[111] Skanda Vivek and Hannah Conner. "Urban road network vulnerability and resilience to large-scale attacks". In: *Safety Science* 147 (2022), p. 105575. ISSN: 0925-7535. DOI: https://doi.org/10.1016/j.ssci.2021.105575. URL: https://www.sciencedirect.com/science/article/pii/S0925753521004173.

[112] Liudong Xing. "Cascading Failures in Internet of Things: Review and Perspectives on Reliability and Resilience". In: *IEEE Internet of Things Journal* 8.1 (2021), pp. 44–64. DOI: 10.1109/JIOT.2020.3018687.

[113] *Report on the Grid Disturbances on 30th–31st July, 2012*. http://cercind.gov.in/2012/orders/Final_Report_Grid_Disturbance.pdf. Central Electricity Regulatory Commission of India. Accessed: 18 February 2024.

[114] Vimal Kishore, Abhijeet R. Sonawane, and M. S. Santhanam. "Manipulation of extreme events on scale-free networks". In: *Phys. Rev. E* 88 (1 July 2013), p. 014801. DOI: 10.1103/PhysRevE.88.014801. URL: https://link.aps.org/doi/10.1103/PhysRevE.88.014801.

[115] Milton Abramowitz and Irene A. Stegun. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. Vol. 55. Applied Mathematics Series. Section 6.6: Incomplete Beta Function. Washington, D.C.: National Bureau of Standards, 1964.

[116] Aric A. Hagberg, Daniel A. Schult, and Pieter J. Swart. "Exploring Network Structure, Dynamics, and Function using NetworkX". In: *Proceedings of the 7th Python in Science Conference*. Ed. by Gaël Varoquaux, Travis Vaught, and Jarrod Millman. Pasadena, CA USA, 2008, pp. 11–15.

[117] Ryan A. Rossi and Nesreen K. Ahmed. "The Network Data Repository with Interactive Graph Analytics and Visualization". In: *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence*. 2015. URL: https://networkrepository.com.

[118] Google. *Google Maps*. https://maps.google.com. Accessed: 2026-03-25. 2026.

[119] Andrej Gajduk, Mirko Todorovski, and Ljupco Kocarev. "Stability of power grids: An overview". In: *The European Physical Journal Special Topics* 223.12 (2014), pp. 2387–2409.

[120] Thomas M. J. Fruchterman and Edward M. Reingold. "Graph drawing by force-directed placement". In: *Software: Practice and Experience* 21.11 (1991), pp. 1129–1164.

[121] Ali Moradi Amani and Mahdi Jalili. "Power Grids as Complex Networks: Resilience and Reliability Analysis". In: *IEEE Access* 9 (2021), pp. 119010–119031. DOI: 10.1109/ACCESS.2021.3107492.

[122] Adilson E. Motter. "Cascade Control and Defense in Complex Networks". In: *Phys. Rev. Lett.* 93 (9 Aug. 2004), p. 098701. DOI: 10.1103/PhysRevLett.93.098701. URL: https://link.aps.org/doi/10.1103/PhysRevLett.93.098701.

[123] Reuven Cohen, Shlomo Havlin, and Daniel ben-Avraham. "Efficient Immunization Strategies for Computer Networks and Populations". In: *Physical Review Letters* 91.24 (2003), p. 247901. DOI: 10.1103/PhysRevLett.91.247901.

[124] Petter Holme and Jari Saramäki. "Temporal networks". In: *Physics Reports* 519.3 (2012), pp. 97–125. DOI: 10.1016/j.physrep.2012.03.001.

[125] Federico Battiston et al. "Networks beyond pairwise interactions: Structure and dynamics". In: *Physics Reports* 874 (2020), pp. 1–92. DOI: 10.1016/j.physrep.2020.05.004.

[126] Franco Scarselli et al. "The Graph Neural Network Model". In: *IEEE Transactions on Neural Networks* 20.1 (2009), pp. 61–80. DOI: 10.1109/TNN.2008.2005605.

[127] M. E. J. Newman. "The structure and function of complex networks". In: *SIAM Review* 45.2 (2003), pp. 167–256. DOI: 10.1137/S003614450342480.

[128] J. Gao, B. Barzel, and A.-L. Barabási. "Universal resilience patterns in complex networks". In: *Nature* 530 (2016), pp. 307–312. DOI: 10.1038/nature16948.

[129] H. J. Herrmann et al. "Onion-like network topology enhances robustness against malicious attacks". In: *Journal of Statistical Mechanics: Theory and Experiment* 2011 (2011), P01027. DOI: 10.1088/1742-5468/2011/01/P01027.

[130] A. Majdandžić et al. "Spontaneous recovery in dynamical networks". In: *Nature Physics* 10 (2014), pp. 34–38. DOI: 10.1038/nphys2819.

[131] A. Majdandžić et al. "Multiple tipping points and optimal repairing in interacting networks". In: *Nature Communications* 7 (2016), p. 10850. DOI: 10.1038/ncomms10850.

[132] Y. Shang. "Robustness of scale-free networks under attack with tunable grey information". In: *EPL (Europhysics Letters)* 95 (2016), p. 28005. DOI: 10.1209/0295-5075/95/28005.

[133] A. Baronchelli, M. Catanzaro, and R. Pastor-Satorras. "Bosonic reaction-diffusion processes on scale-free networks". In: *Physical Review E* 78 (2008), p. 016111. DOI: 10.1103/PhysRevE.78.016111.

[134] N. Masuda, M. A. Porter, and R. Lambiotte. "Random walks and diffusion on networks". In: *Physics Reports* 716–717 (2017), pp. 1–58. DOI: 10.1016/j.physrep.2017.07.007.

[135] D. Aldous and J. A. Fill. *Reversible Markov Chains and Random Walks on Graphs*. Unfinished monograph, recompiled 2014. Available at https://www.stat.berkeley.edu/users/aldous/RWG/book.html. 2002.

[136] S. Majhi, S. Rakshit, and D. Ghosh. "Oscillation suppression and chimera states in time-varying networks". In: *Chaos* 33 (2023), p. 053107. DOI: 10.1063/5.0054291.

[137] A. Saha et al. "Extreme events in coupled systems with quenched disorder". In: *Physical Review E* 95 (2017), p. 062219. DOI: 10.1103/PhysRevE.95.062219.

[138] P. Chaurasia and S. Sinha. "Extreme events and intermittent chaos on networks with nonlinear diffusion". In: *Physical Review E* 109 (2024), p. 014217. DOI: 10.1103/PhysRevE.109.014217.

[139] Y. Kuang. *Delay Differential Equations with Applications in Population Dynamics*. Boston, MA: Academic Press, 1993. ISBN: 9780124276802.

[140] T. Erneux. *Applied Delay Differential Equations*. Vol. 3. Surveys and Tutorials in the Applied Mathematical Sciences. New York, NY: Springer, 2009. DOI: 10.1007/978-0-387-74372-1.

[141] J. K. Hale and S. M. V. Lunel. *Introduction to Functional Differential Equations*. Vol. 99. Applied Mathematical Sciences. New York, NY: Springer, 1993. DOI: 10.1007/978-1-4612-4342-7.

[142] C. W. Gardiner. *Stochastic Methods: A Handbook for the Natural and Social Sciences*. 4th. Springer Series in Synergetics. Berlin: Springer, 2009. ISBN: 9783540707127.

[143] N. G. van Kampen. *Stochastic Processes in Physics and Chemistry*. 3rd. Amsterdam: North-Holland, 2007. ISBN: 9780444529657.

[144] H. Risken. *The Fokker–Planck Equation: Methods of Solution and Applications*. 2nd. Vol. 18. Springer Series in Synergetics. Berlin: Springer, 1989. DOI: 10.1007/978-3-642-61544-3.

[145] H. A. Kramers. "Brownian motion in a field of force and the diffusion model of chemical reactions". In: *Physica* 7 (1940), pp. 284–304. DOI: 10.1016/S0031-8914(40)90098-2.

[146] S. H. Strogatz. *Nonlinear Dynamics and Chaos*. Reading, MA: Addison-Wesley, 1994. ISBN: 9780738204536.

[147] S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes. "Critical phenomena in complex networks". In: *Reviews of Modern Physics* 80 (2008), pp. 1275–1335. DOI: 10.1103/RevModPhys.80.1275.

[148] V. Dakos et al. "Methods for detecting early warnings of critical transitions in time series illustrated using simulated ecological data". In: *PLOS ONE* 7 (2012), e41010. DOI: 10.1371/journal.pone.0041010.

[149] M. Kivelä et al. “Multilayer networks”. In: *Journal of Complex Networks* 2 (2014), pp. 203–271. DOI: 10.1093/comnet/cnu016.

[150] S. Boccaletti et al. “The structure and dynamics of multilayer networks”. In: *Physics Reports* 544 (2014), pp. 1–122. DOI: 10.1016/j.physrep.2014.07.001.

[151] W. Feller. *An Introduction to Probability Theory and Its Applications*. 3rd. Vol. 1. New York, NY: Wiley, 1968. ISBN: 9780471257080.