FAILURE MITIGATION, VULNERABILITY DETECTION AND PERSISTENCE OF NETWORK FLOWS IN COMPLEX SYSTEMS

By

Alaa Moussawi

A Dissertation Submitted to the Graduate Faculty of Rensselaer Polytechnic Institute in Partial Fulfillment of the Requirements for the Degree of DOCTOR OF PHILOSOPHY

Major Subject: PHYSICS

Examining Committee:

______________________________
György Korniss, Dissertation Adviser

______________________________
Boleslaw Szymanski, Dissertation Adviser

______________________________
Vincent Meunier, Member

______________________________
Joel Giedt, Member

Rensselaer Polytechnic Institute
Troy, New York

April 2018
(For Graduation May 2018)
# CONTENTS

LIST OF TABLES ......................................................... vii
LIST OF FIGURES ....................................................... viii
ACKNOWLEDGEMENTS .................................................. xiv
ABSTRACT ................................................................. xvi

1. BACKGROUND ....................................................... 1

2. CASCADING FAILURES IN SPATIALLY-EMBEDDED DISTRIBUTED FLOW NETWORKS ..................................................... 6
   2.1 Literature Review ................................................... 6
   2.2 Introduction ...................................................... 10
   2.3 Methods .......................................................... 12
      2.3.1 Distributed Flow ............................................ 12
      2.3.2 Cascade Model ............................................ 14
      2.3.3 Empirical Network ....................................... 14
      2.3.4 Network Models .......................................... 14
      2.3.5 Outlier Removal ........................................... 15
   2.4 Main Results .................................................... 15
      2.4.1 Stochastic Capacity Allocations ........................... 16
      2.4.2 Sensitivity to Target Selection in Spatially-Localized Multi-Node Attacks ........................................... 18
      2.4.3 \( N \)-Stable and \((N-1)\)-Stable Capacity Allocation for the UCTE network ............................................ 20
      2.4.4 Multi-node Attack Strategies ............................... 24
      2.4.5 Phase Transitions in Cascading Failures ................... 26
      2.4.6 Cascade-size Distribution Analysis ....................... 28
      2.4.7 Predicting the Severity of Cascading Failures ............. 30
   2.5 Further Findings ................................................ 31
      2.5.1 UCTE Network Properties .................................. 31
      2.5.2 Analysis of Optimal Stochastic Capacity Allocation Characteristics ............................................. 32
      2.5.3 Non-monotonic Behavior Under Spatially-Correlated Attacks ........................................... 33
2.5.4 Node Sensitivity in Random Geometric Graphs (RGGs) and Scale-Free Networks ................................................. 34
2.5.5 Failure Response in $N$-Stable and $(N-1)$-Stable Networks .... 35
2.5.6 Efficacy of Stochastically Generated Capacity Allocations ... 56
2.5.7 Greedy and Spatially Correlated Attack Strategies ............. 58
2.5.8 Cascade Severity Measures ($G$ and $S$) .......................... 59
2.5.9 Analysis of First and Second Largest Giant Components .... 60
2.5.10 Failures Near the Phase Transition ............................. 62
2.5.11 Correlations in Single and Multi-Node Failures ............... 65
2.6 Conclusion ..................................................................... 72
3. ANALYSIS OF ANOMALIES IN THE DISTRIBUTION GRID .... 77
  3.1 Anomaly Detection and Classification .............................. 77
    3.1.1 Background ...................................................... 77
    3.1.2 Plan ............................................................... 78
    3.1.3 Data Resourcing ................................................. 79
    3.1.4 Anomaly Detection ............................................. 79
    3.1.5 Anomaly Classification ........................................ 81
  3.2 Recovery of Dynamical System Parameters ...................... 83
    3.2.1 Methods ......................................................... 83
    3.2.2 Optimal Recovery Interval ................................... 84
    3.2.3 Evolution of Dynamical System ............................. 87
    3.2.4 Granularity Vs. Recovery Window ......................... 89
    3.2.5 Performance on Modeled Data .............................. 94
4. PERSISTENCE IN NETWORKS ........................................ 98
  4.1 Introduction .................................................................... 98
  4.2 Persistence in Diffusive Models ..................................... 100
    4.2.1 Diffusion on Erdős-Rényi Graphs .......................... 101
  4.3 Persistence in Contact Processes ................................... 102
    4.3.1 Contact Processes on Erdős-Rényi Graphs ............... 105
  4.4 Complete Graphs ..................................................... 108
  4.5 Conclusions .................................................................. 108
5. CONTRIBUTIONS AND FURTHER RESEARCH .................. 110
  5.1 Future Research ........................................................ 111
  5.2 Contributions ............................................................ 112
APPENDICES ................................................................. 114

A. Probability Estimation and Parameter Recovery in Stochastic Dynamical Systems ........................................ 114
   A.1 Parameter Recovery ................................................. 114
   A.2 Probability Estimation ............................................ 115

B. Steady-State Behavior of the SIS Model Through Mean Field Approximation .............................................. 116
   B.1 Loss of Persistent Sites in SIS model ......................... 116
   B.2 Fluctuations about the Endemic State ....................... 117

REFERENCES ............................................................... 119
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Critical Exponent (total crossings) as a Function of $\gamma$ for a contact</td>
<td>104</td>
</tr>
<tr>
<td></td>
<td>process on a one-dimensional lattice with 10,000 sites, run for a total of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10,000 iterations.</td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td>Critical Exponent (upwards crossings) as a Function of $\gamma$ for a contact</td>
<td>104</td>
</tr>
<tr>
<td></td>
<td>process on a one-dimensional lattice with 10,000 sites, run for a total of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10,000 iterations.</td>
<td></td>
</tr>
<tr>
<td>4.3</td>
<td>Critical Exponent (downwards crossings) as a Function of $\gamma$ for a contact</td>
<td>104</td>
</tr>
<tr>
<td></td>
<td>process on a one-dimensional lattice with 10,000 sites, run for a total of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10,000 iterations.</td>
<td></td>
</tr>
</tbody>
</table>
LIST OF FIGURES

2.1 Cascades on the UCTE network triggered by the removal of a single (highest load) node. (a) The cascade size as a function of tolerance parameter for (a) uniform capacity allocation; (b) stochastic capacity allocation of varying $\sigma$ values: $\sigma = 0.25$ (green), $\sigma = 0.50$ (blue), and $\sigma = 1.00$ (red), with 100 simulations for each case. For comparison, the black connected data points show the performance of the uniform capacity allocation presented in (a). (c) Visualization of the damage caused in the UCTE power grid by the removal of the highest load node using the identical (uniform) capacity allocation vs. the best-case and worst-case scenario of the stochastic capacity allocations. (d) Correlation analysis of load/node degree vs. excess capacity for the best-case and worst-case scenario stochastic capacity allocations.

2.2 Node sensitivity in the UCTE network. (a) $G$ vs. $\sum_i \ell^\text{initiator}_i$ (b) $G$ vs. $\sum_i e^\text{initiator}_i$ (c) Contour plot of $2r$ region (d) Contour plot of $3r$ region (e) Visualization of variability for small changes in the target set for spatially-clustered attacks on the UCTE network. Case 1 and Case 2 visualize the avalanche of failed nodes (blue) triggered by the removal of two distinct sets of nine-spatially-localized-nodes (red) from the same $2r$ region, with $\alpha = 0.1$.

2.3 Spatially-concentrated and distributed (random) attacks in $N$-stable and $(N-1)$-stable UCTE networks. For each $n$ there are 5 realizations of random attacks. The tolerance parameter of the $N$-stable system is $\alpha = 0.5927$, and for the $(N-1)$-stable $\epsilon = 0.1$. (c) Visualization of $1r$ (red circle) and $2r$ (blue circle) regions used for spatially localized attacks in the UCTE network, where the distance is calculated from the geographic center of the network (red dot).

2.4 Multi-node attacks on $N$-stable and $(N-1)$-stable UCTE networks. (a) nine-random-node removal from the $2r$ region; (b) nine-random-node removal from the entire network; (c) nine-center-node removal with stochastic capacity allocation; (d) nine-highest-load-node removal with stochastic capacity allocation. Each scenario contains 500 repetitions on the $N$-stable ($\alpha = 0.5927$) and $(N-1)$-stable ($\epsilon = 0.1$) UCTE network. (e) Comparison of stochastic search for optimal capacity allocation (red circle) with uniform capacity allocation (black line) for nine-center-node attacks on the $N$-stable UCTE network with $\alpha = 0.5927$ over 500 trials. (f) Comparison of stochastically optimized (red circle) and non-optimized uniform (black circle) capacity allocations against various tightly-clustered nine-node attacks with 1230 repetitions.
2.5 Severe attack patterns in the $N$-stable UCTE network. (a) Size of the surviving giant component $G$ as a function of the total load of targeted nodes. The data points on the continuous lines represent the sizes of the total load of the targeted nodes; the lines show the sizes of $G$ when targeting those nodes. Their color codes identify the attack pattern used: the four-highest-load-node removal (purple), the single node that individually causes the greatest damage, nodes selected by our greedy algorithm (green), the 4 nodes causing the highest damage when individually removed (blue). (b) Comparison of the size of damage caused by various attack patterns by ranking $G$ in nondecreasing order. 300 simulations for each attack scenario on the $N$-stable UCTE network with $\alpha = 0.5927$. (c) Visualization on the UCTE network of the nodes used in the different attack patterns for triggering the cascading failures.

2.6 Phase transitions with increasing protection in UCTE and RGG networks. (a) four-center-node removal in $N$-stable UCTE network. (b) nine-center-node removal in $(N-1)$-stable UCTE network. (c) four-center-node removal in $N$-stable UCTE network. (d) four-center-node removal in $(N-1)$-stable UCTE network. (e) 3 different RGG networks of identical size $N = 1000$ and average degree $\langle k \rangle = 10$; (f) 4 realizations of RGGs $\langle k \rangle = 10$, of different system sizes. The inset shows the second largest component ($G_2$) sizes for the corresponding networks.

2.7 Power-law tail of cascade size distributions in the phase transition regime. (a) Power-law fit (red line) of four-clustered-node removals (black dots) with $\alpha = 0.6$. (b) Power-law fit (red line) of four-random-node removals (black dots) with $\alpha = 0.6$. (c) Power-law fit of four-clustered-node removals (black dots) with $\alpha = 0.8$. (d) Power-law fit (red line) of four-random-node removals (black dots) with $\alpha = 0.8$. Small event regime $1 \leq S \leq 200$, large event regime: $201 \leq S \leq 300$ (e) Power-law trend of cascade size distributions for random single-node removal in RGGs of different systems sizes and $\langle k \rangle = 10$ for $\alpha = 0.45$ and (f) $\alpha = 0.50$.

2.8 Correlation analysis of failures triggered by the failure of 4 nodes on the UCTE network. $\alpha = 0.5927$ (relative tolerance); 300 repetitions of four-random-node failures from the entire network.

2.9 Properties of the UCTE network. (a) Node degree distribution; (b) correlation between node degree and node load; (c) histogram of link length distribution.

2.10 Node sensitivity of single-node removal in the UCTE network. The color hue indicates the size of damage (surviving giant component) when that single node fails.
2.11 Comparison of best-case and worst-case excess capacity allocations as a function of node degree in the UCTE network. $\Delta C_i$ vs. $K_i$ for (a) Best-case for $\alpha = 0.40$, (b) worst-case for $\alpha = 0.40$, (c) best-case for $\alpha = 0.45$, (d) worst-case for $\alpha = 0.45$. ................................. 46

2.12 Comparison of best-case and worst-case excess capacity allocations as a function of initial state node load in the UCTE network. $\Delta C_i$ vs. $\ell_i$ for (a) Best-case for $\alpha = 0.40$, (b) worst-case for $\alpha = 0.40$, (c) best-case for $\alpha = 0.45$, (d) worst-case for $\alpha = 0.45$. ................................. 47

2.13 Comparison of best-case and worst-case excess capacity allocations in the UCTE network. (a) Comparison of excess capacity, normalized by initial state load, as a function of node degree for $\alpha = 0.40$ and $\alpha = 0.45$. (c) Comparison of excess capacity, normalized by initial state load, as a function of initial state node load for $\alpha = 0.40$ and (d) $\alpha = 0.45$. 48

2.14 Comparison of best-case and worst-case excess capacity allocations by node ID in the UCTE network. (a) Best-case for $\alpha = 0.40$, (b) worst-case for $\alpha = 0.40$, (c) best-case for $\alpha = 0.45$, (d) worst-case for $\alpha = 0.45$. 49

2.15 Comparison of UCTE network with uniform capacity allocation (left) and UCTE network with stochastic best-case capacity allocation (right). (a-b) Node sensitivity for single node failure. The red line highlights the averaged value of the data points. (c-d) Node sensitivity for single node failure rank ordered by the size of surviving giant component. (e-f) Histograms visualizing the distribution of the size of surviving giant component for single node failures. ................................. 50

2.16 Non-monotonic behavior in spatially-correlated attacks in the UCTE network vs the tolerance. We trigger the cascades by removing the same set of 9 nodes (red) from the 1r region in the UCTE network for two different tolerance ($\alpha$) values. We show that a smaller tolerance parameter leads to a smaller damage (left), whereas a higher tolerance parameter of $\alpha = 0.15$ (right) causes a larger cascading failure. This result suggests the presence of fuse nodes, which can prevent the spreading of cascades in case they fail due to a lower capacity allocation. . . 51

2.17 Node sensitivity analysis for single node removal. The subfigures plot the size of the surviving giant component (in case the cascade is triggered by the removal of a single node) as a function of node load in (a) scale-free (SF) network with system size $N = 1000$ and $\langle k \rangle = 3$, (b) UCTE network, (c) scale-free (SF) network with system size $N = 1000$ and $\langle k \rangle = 10$; (d) RGG with system size $N = 1000$ and $\langle k \rangle = 10$. Each network is constructed with $\alpha = 0.45$ tolerance parameter. ................................. 52
2.18 Sample-to-sample fluctuation and finite-size behavior of cascading failures on RGGs. Cascades triggered by the removal of the highest load node on RGG networks of size (a) $N = 1000$, (b) $N = 2000$, (c) $N = 10000$, with 3 different realizations for each system size. (d) Analysis of non-monotonic behavior scaling with system size. Simulations performed on synthetic random geometric graphs (RGGs) of average degree $\langle k \rangle = 10$ and various $N$ system sizes.

2.19 Required capacity comparison for $N$-stable and $(N{-}1)$-stable UCTE network constructions.

2.20 Nine-random-node removals from $2r$ region for (a) $N$-stable and (b) $(N{-}1)$-stable UCTE network.

2.21 Stability of $N$-stable and $(N{-}1)$-stable UCTE networks against multi-node attacks. The two blue nodes on the UCTE network visualization depict critical nodes (fuses) that increase the damage in the system in the case where they survive.

2.22 Stochastic capacity allocation optimization for $N$-stable UCTE network. The red data points depict the stability of the (a) $N$-stable UCTE networks against 9 random node removal from the entire network. (b) Trials ordered by $G$. The green data points highlight the vulnerability of the network, if we add on top of the initial capacity allocation the best stochastic capacity allocation against 9 center node removals.

2.23 Greedy selection of (a) 2 most damaging nodes with every other node; (b) 3 most damaging nodes with every other nodes. The green lines represent the size of surviving giant component in case of the removal of the (a) 2 most damaging nodes only; (b) the 3 most damaging nodes only. Simulations performed on $N$-stable UCTE network with $\alpha=0.5927$.

2.24 Five-center-node attack. From the 9 center nodes we attack 5 different nodes for each simulation, leading to 126 possible combinations. Simulations performed on $N$-stable UCTE network (black) with $\alpha=0.5927$ and $(N{-}1)$-stable UCTE network (red) with $\epsilon=0.1$.

2.25 Correlation analysis of $S$ vs. $G$. $S$ represents the number of failed nodes throughout the cascade process, whereas $G$ is the size of surviving giant component. In order to quantify the same information (size of damage), we plot the $1-G$ that is the fraction of failed nodes. (a) The severity of single node removal; (b) severity of 4 spatially clustered node removals. Simulations performed on $N$-stable UCTE network with $\alpha = 0.5927$.

2.26 Comparison of the largest and second largest surviving giant component ($G_1$ and $G_2$) in RGGs.
2.27 Comparison of surviving giant component and second largest surviving component. (a) The surviving giant component in ranked order, (b) the second largest component in ranked order, as each single node in the UCTE network is individually attacked, with a capacity threshold $\alpha = 0$. (c) The surviving giant component size ($G_1$) and second largest component size ($G_2$) as a function of capacity threshold $\alpha$ under a 4 center node attack on the UCTE network. A phase transition is visible.

2.28 Power-law trend around the phase transition region in $N$-stable UCTE network. Comparison shown for 4 random node removal and 4 clustered node removal for various $\alpha$ values: below ($\alpha = 0.6$), around ($\alpha = 0.8$) and above ($\alpha = 1.2$) the phase transition region.

2.29 Power-law trend around the phase transition region in RGG network of size $N = 1000$ and $\langle k \rangle$. Cascades triggered by the removal of single nodes for various $\alpha$ values: below ($\alpha = 0.15$), around ($\alpha = 0.45$ and $\alpha = 0.50$) and above ($\alpha = 0.65$) the phase transition region.

2.30 Power-law fits around the phase transition region in RGG networks of various system sizes and $\langle k \rangle = 10$. Cascades triggered by the removal of single-nodes for various $\alpha$ values: at the critical region ($\alpha = 0.45$) and beyond ($\alpha = 0.50$).

2.31 Correlation between surviving giant component sizes for all possible single node attacks on the UCTE network with two $N$-stable capacity thresholds as represented on the axes.

2.32 Correlation analysis of multi-node attacks and the sum of individual damage each initiator node induces in $N$-stable UCTE network (small-range).

2.33 Correlation analysis of multi-node attacks and the sum of individual damage each initiator node induces in $N$-stable UCTE network (mid-range).

2.34 Correlation analysis of multi-node attacks and the sum of individual damage each initiator node induces in $N$-stable UCTE network (large-range).

2.35 Correlation analysis of failures triggered by the removal of a set of 4 nodes. $\alpha = 0.5927$ (relative tolerance); 300 repetitions of four-random-node removals from the entire network.
2.36 Comparison of four-clustered and four-random-node removals. Subfigures (a) and (b) present the size of the surviving giant component for the four-clustered-node removals as the function of the total node degrees $\sum k$ of the initiator nodes, as well as the total load $\sum \ell$ of initiator nodes. All simulations are performed on UCTE network with $\alpha = 0.60$.

2.37 Average $G$ vs $\alpha$ of four-random-node failures in the UCTE network.

3.1 Five principal variables of the power transmission system.

3.2 Number of data points $n$, against $L^2$-norm of difference of recovered matrices $A$, where matrices are recovered from two consecutive data samples $i_{A1} \in [0, i]$ and $i_{A2} \in [i, 2i]$ for time-steps of 1 and 2.

3.3 Number of data points $n$, against $L^2$-norm of difference of recovered matrices $A$.

3.4 Identical to Fig. 3 (a, b) with $L^2$-norm($\Delta A$) replaced with $L^\infty$-norm($\Delta A$). Refer to caption of figure 3.

3.5 Measuring the change in $A$ as a function of time.

3.6 $L^2$-norm($\Delta A$) as a function of time for a fixed maximum time interval $T$, and varying time-steps $\Delta t$. Number of data points used will vary.

3.7 $L^2$-norm($\Delta A$) as a function of time for a fixed maximum time interval $T$, and varying time-steps $\Delta t$. Magnified version of Fig. 6.

3.8 $L^2$-norm($\Delta A$) as a function of time for a fixed maximum time interval $T$, and varying time-steps $\Delta t$. Magnified version of Fig. 6 and Fig. 7.

3.9 Time span necessary to accurately recover matrix $A$ measured in units $n^*$ (period of data sample used) against the time-step $\Delta t$ (same unit scale).

3.10 Change in $A$ over labeled time spans over 5 minute intervals as measured by $L^2$-norm($\Delta A$). Replicated methods used in Fig. 5, with 1500 data point span used for recovery of matrix $A$.

3.11 The slope of $L^2$-norm($\Delta A$) vs $n$ (slope of Fig. 8).

3.12 $\varepsilon$ vs. $\Delta t_2$ for $\Delta t_1 = 1$.

3.13 $L^2$-norm($\Delta A$) vs. $\Delta t$, showing a minimum for $\Delta t = 18$.

3.14 $\varepsilon$ vs. $n$, for different values of $\Delta t_2$ in each subfigure.

3.15 Measuring $L^2$-norm($\Delta A$).
4.1 Total persistence, $P_i(t)$ for diffusion on a 1-D chain as a function of time (log-log scale). System initialized by *uniform distribution* with varying spreads as indicated by the legend. .............................................. 101

4.2 Total persistence, $P_i(t)$ for diffusion on a 1-D chain as a function of time (log-log scale). System initialized by *Gaussian distribution* with varying standard deviations as indicated by the legend. ......................... 102

4.3 Total persistence for diffusion on a 2-D chain as a function of time (log-log scale). System initialized by *uniform distribution* with varying spreads as indicated by the legend. .............................. 103

4.4 Total persistence for diffusion on an Erdős-Rényi Graph as a function of time (log-log scale). System initialized by *uniform distribution*. Persistence is evaluated for nodes of a particular degree. Run for 2 system sizes, $N = 1000$ and $N = 10,000$ ........................................ 105

4.5 Total persistence of a contact process on a 1-D lattice $P_i(t)$ as a function of time (log-log scale). 10,000 lattice sites, 10,000 iterations, and time scale $dt = 0.01$. ................................................................. 106

4.6 Up-crossing persistence of a contact process on a 1-D lattice $P_i^+(t)$ as a function of time (log-log scale). 10,000 lattice sites, 10,000 iterations, and time scale $dt = 0.01$. ................................................................. 106

4.7 Down-crossing persistence of a contact process on a 1-D lattice $P_i^-(t)$ as a function of time (log-log scale). 10,000 lattice sites, 10,000 iterations, and time scale $dt = 0.01$. ................................................................. 107

4.8 Up-crossing, down-crossing, and total persistence for a contact process on an Erdős-Rényi graph as a function of time (Semi-Log scale). System initialized with *uniform distribution*. ............................................. 107

4.9 Up-crossing, down-crossing, and total persistence on Complete graphs (semi-log scale). ................................................................. 109

4.10 Up-crossing, down-crossing, and total persistence on Complete graphs (semi-log scale). ................................................................. 109
I would like to take the opportunity to acknowledge those who greatly assisted me over the past five years in my growth and learning. First I would like to thank my advisors György Korniss and Boleslaw Szymanski who were patient and allowed me the opportunity to learn a diverse set of skills while providing the support necessary for me to gain those skills to pursue an endeavor I was ill prepared for. Their guidance and direction has tremendously impacted my future career goals, and has shown me the limits as well as the successes of research, and more importantly, how reproducible research is conducted. Without their kindness and support, I would not have enjoyed a great graduate school experience and could have never reached this point. On a similar note, I would like to thank my friends and colleagues Panagiotis Karampourniotis, Noemi Derzsy, Xin Lin, and Xiang Jiu who were most helpful, and who always were willing to offer their time and assistance when I had questions or concerns. They were not only academic resources, but personal resources who I discussed life plans and career aspirations with, and friends who I hope to keep strong ties with into the future.

In addition I would like to thank Scott Backhaus, Marc Vuffray, and Andrey Lokhov from the Center for Non-linear Studies at Los Alamos National Laboratories. Without their guidance, I would not have had the opportunity to learn and perform research on the distribution grid, giving me an introduction to how research is performed in a non-academic setting.

And of course, without the professors at Rensselaer Polytechnic Institute this endeavor would have never been possible. I would like to thank professor Vincent Meunier (committee member), who gave me a crash course into computational modeling in the computational physics course, professor Joel Giedt (committee member) who eloquently showed how physicists approach a problem they have not yet solved in the course titled Electrodynamics, and professor John Schroeder, who in addition to instructing me in statistical mechanics, shared many intriguing life stories dating back to WWII and the 1940s.
I must also express my love and gratitude to my brother Ali Moussawi, without whom I would have likely never pursued this degree, and who was relentlessly supportive of my endeavors, and my sister Souad Moussawi who was extremely supportive throughout the past 5 years as well. I would also like to thank my mother and father, who have been unknowingly pivotal in providing a childhood environment allowing me to grow and pursue my desires.

In addition, I would like to express thanks to my good friend Karamchandra Rampersaud who was intelligent beyond his time, and who taught me important life lessons that have helped me over the years. I would also like to thank Andrea Oliver, Angelia Vargas, Marly Vargas, Andrew Badana, and Gustavo Vasquez, with whom I have maintained great ties with over the many years I have spent away from our hometown, and who have always provided me with support.

This work was supported in part by the Defense Threat Reduction Agency (DTRA) Award No. HDTRA1-09-1-0049, the Defense Advanced Research Projects Agency (DARPA) and the Army Research Office (ARO) under Contract No. W911NF-17-C-0099, by the Office of Naval Research Grant No. N00014-15-1-2640 and the Army Research Laboratory under Cooperative Agreement Number W911NF-09-2-0053 (the ARL Network Science CTA). The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.
ABSTRACT

Complex systems arise in many environments, and can be useful in modeling many aspects of physical and social systems. For many applications the maintenance and operation of these systems is poorly understood. We study the transmission and distribution grids as networks, and we investigate their temporal evolution, including the spread of cascades on such systems. We also analyze the occurrence of anomalies and future outcomes of such anomalies in the distribution grid. In addition, we investigate the persistence of states in lattice systems and networks.

Cascading failures are a critical vulnerability of complex information or infrastructure networks, and are particularly difficult to analyze in the transmission grid. We investigate the properties of load-based cascading failures in real and synthetic spatially-embedded network structures which can be seen as generalizations of power grids, and propose mitigation strategies to reduce the severity of damages caused by such failures. We introduce a stochastic method for optimal heterogeneous distribution of resources (node capacities) subject to a fixed total cost. Additionally, we design and compare the performance of networks with $N$-stable and $(N-1)$-stable network.capacity allocations by triggering cascades using various real-world node-attack and node-failure scenarios. We show that failure mitigation through increased node protection can be effectively achieved against single-node failures. However, mitigating against multiple node failures is much more difficult due to the combinatorial increase in possible sets of initially failing nodes in addition to the strongly non-linear dependence of cascade size on the set of initially targeted nodes. We analyze the robustness of the system with increasing protection, and find that a critical tolerance exists at which the system undergoes a phase transition, and above which the network almost completely survives an attack. Moreover, we show that cascade-size distributions measured in this region exhibit a power-law decay indicating that this region holds a critical value. Finally, we find a strong correlation between cascade sizes induced by individual nodes and sets of nodes. We also show that network topology alone is a weak predictor in determining the
progression of cascading failures.

On a less theoretical yet more applicable note, we study anomaly occurrences in the distribution grid. We utilize data harvested from phasor measurement units (PMUs) in the distribution grid. The department of energy (DOE) placed these remote sensors in various locations throughout the distribution grid in the past decade in an effort to improve the monitoring, resilience, and efficiency of maintenance, in the distribution grid. The first task is to identify the occurrence of anomalies in the data set. This is performed through a statistical measure indicating the likelihood of an incoming signal. Next the data is classified into one of nine expert-identified classes. Learning algorithms are then trained on this data set that has been labeled by the expert. The performance of the model is investigated.

Finally, the persistence of states is studied in various systems under the respective system dynamics. Lattices in one and two dimensions as well as Complete and Erdős-Rényi graphs are investigated. A contact process and diffusion process are applied to these networks, and the evolution of persistence (being the probability that a site remains in the same state until time $t$) is investigated. We find the expected and theoretically backed results known in the literature for one and two dimensional lattices. We find non-trivial behavior in Erdős-Rényi graphs, and find the expected trivial behavior in Complete graphs. Interestingly, we find that when certain conditions are met, the persistence found for diffusive models and for contact processes yield the same critical decay exponent, suggesting that there are underlying dynamics governing the persistence of the system that are not entirely controlled by the model dynamics.
CHAPTER 1
BACKGROUND

In the current era of globalization we face an expansive set of complex issues concerning the proliferation of an already vast population. Many of these issues correspond with emergent statistical properties visible for large system sizes. This elucidates the need for understanding the behavior of complex systems arising from social, economic, or physical human interactions, as well as the effects that these systems may have on neighboring systems. My research efforts focus on analyzing such properties by utilizing network models in coordination with scientifically motivated computational methodologies to understand their temporal evolution and controllability. Applications have ranged from modeling and analysis of power grids, machine learning on distribution grid sensor data, network evolution and controllability analysis of the global risks network, to agent based modeling of economic systems and their emergent wealth distributions. The common goal is to achieve a mathematical understanding of such systems and their evolution, and to increase their resilience. In addition to scientific discoveries, the impact of such work could range from smart advertising, scientifically informed policy making, to an improved understanding of crowd psychology.

Networks or compound networks can adequately model a range of complex systems. A common vulnerability of such systems is that an individual failure can induce a chain of consequential failures. Such effects can be observed in infrastructure networks [1], [2], urban micro-grids [3], commuter transportation and mobility networks [4], [5], [6], financial systems [7], and biological networks [8]. The common denominator is that their complexity and susceptibility to failure both increase with network size. Coupled with the observation that the sizes of these networks are increasing in proportion to the global population, concerns about the stability of these systems and our understanding of their robustness naturally arise. The scientific community has acknowledged the importance of studying the resilience of networks, and efforts are underway to unearth how processes can be controlled and
their evolution optimized either with driving functions or by altering the characteristics of the networks [9], [10]. In the case of spatially embedded networks, cascading failures can be particularly detrimental, yet are poorly understood [11]. They can cause outages that last for extended durations over large regions. Such outages can disrupt economic systems, transportation networks, and communication networks, in addition to aggravating effects that modern societies cannot cope with over long periods. One notable instance was the 2003 Northeast blackout [1], where a power failure triggered in Ohio cascaded into Ontario and back down through the US disrupting power service all over the north east and costing the US an estimated 6 billion dollars, causing 11 deaths, and disrupting the lives of millions of Americans.

In research performed at Rensselaer Polytechnic Institute, I found that power grids are currently operating at or near critical capacity (sum of allocated network resources) as power demands are approach this capacity. With increasing population size driving higher energy demands on old infrastructure, grid operation at this critical phase is highly unstable. My research has found that the distribution of cascade (failure) sizes exhibits a power-law tail (at the critical operational region), indicating that current capacity allocations are in a phase transition region. The research also revealed an abrupt increase in system resilience across the phase transition region as total grid capacity is increased, further supporting the claim. These results necessitate a stronger understanding of power system dynamics to reliably and effectively utilize the power grid at this critical phase, as energy demands increase.

As part of my doctoral research I have also investigated the relationship between the progression of cascades induced by single-node failures and multi-node failures. My research revealed that the propagations of cascades induced by multiple nodes are similar to the cascades induced individually by the single most damaging node from the set. This correlation weakens as the set of nodes initiating the cascade grows. My research has also investigated cascade mitigation, showing that current industry standard capacity allocation schemes ($N - k$ stable capacities) are non-optimal for many classes of failures. Stochastic variations upon these capacity schemes have proven capable of improving network resiliency, again emphasizing the
need for a stronger understanding of AC power system dynamics. This work was supported in part by DTRA and ARL and was published in Scientific Reports [11].

Similar to the main power grid, distribution grids experience various issues on the local scale. At Los Alamos National Labs I investigated how distribution grid resilience, maintenance, and operation could be improved using recently introduced sensor technologies. Over recent years the Department of Energy has installed PMUs (Phasor Measurement Units) in various locations throughout the distribution grid, with the aim of monitoring the state of distribution nodes. I was given the opportunity to analyze the data collected by these PMUs. The effort was two-fold. First, identifying anomalies in real time; second, classifying them. To identify anomalies we assume that the local dynamics of the distribution grid can be approximated as a stochastic linear dynamical system. Taking previous time steps as a prior on incoming signals, we compute the probability of the incoming signal. Once anomalous signals are identified they are classified by one of many learning algorithms. Our findings show that the most effective algorithm is the neural network, trained on a set of features that were manually engineered to help distinguish between the various classes of anomalies. Results were successful, showing the capability to improve resiliency and efficiency of maintenance in the distribution grid. The DOE has approved the project for further sponsorship and the material has been handed to another researcher who is currently at LANL.

While the main focus has thus far been on power and distribution grids, the effects of such failures are not localized and can spill into other domains. Effects from power outages can induce economic loss, governance failure and a host of other detrimental effects, particularly in urban environments. This is true of most large-scale network failures. For instance, epidemics can disrupt the workflow of large regions, resulting in traffic bans such as those during the Ebola scare, destabilizing economies and disrupting standard urban function. A scientific understanding of the interplay of these networks is essential for a proper analysis of global stability. For this reason the World Economic Forum (WEF) analyzes the state of global risks by crowdsourcing the opinions of experts, to construct a publicly available and annually updated description of the state of our world. The aim is to facilitate
an understanding of the progression of global risks, and to aid scientists in their investigations by providing a common framework that can be used as a basis for scientific models.

Szymanski et. al. [12] developed a predictive model specifically for the goal of understanding the evolution of global risks as defined by the WEF. The model considers each risk as an individual node that can trigger other risks with Poisson distributed probabilities. The relative intensities of these probabilities are deduced by expert assessments, and their absolute intensities are obtained through maximum likelihood estimation by training on historical data. We have utilized this model to understand the asymptotic trajectory of the global risks from a particular point in time. We also investigated the theoretical limits of the predictive accuracy of the system as a function of time through Monte Carlo simulation, similar to what has been suggested by Microsoft Research (Hofman et. al.). We also investigated how the network can be optimally forced (driven) to a favorable steady state (where all risks are inactive) under fixed cost. Combining elements of control theory and network science has been fruitful, and the research has revealed the conditions necessary to achieve controllability of a network with a finite amount of energy (network costs), and how to compute the necessary driving functions for networks governed by linear dynamics. The current focus of our research is on applying similar methodologies to non-linear systems by iteratively linearizing them. We have successfully computed optimal driving functions for the non-linear global risks model. Our methodologies are mathematically generalizable, and future goals include the application of controllability to epidemiological models, as well as implementing efficient scaling of our algorithms.

The focus has thus far been on research applications relevant to real world systems where we utilize real network data and model future outcomes. We now consider the study of persistence of nodes within networks from a theoretical perspective. We utilize Monte-Carlo simulations to gain insight into how long opinions or field values retain their initial state in a network. In other words, we define the persistence of a system to be the probability that a site remains in its initial state till time $t$, a definition which can be extended to continuous variables. This inves-
tigation of "first-passage" times can be held in a physical setting where diffusion occurs. One relevant question pertaining to the physical setting is "how long will it take for a customer to smell the food they have ordered once it has been cooked and the smell has began to diffuse throughout the air"? Such questions can not be answered deterministically, but instead can be gauged probabilistically through the use of their underlying distributions. We verify findings for diffusion found in the literature for lattice models, and extend our work to encompass random graphs. We also study persistence in contact process on various graph structures in hopes of identifying universality classes common to fixed topologies, under different spreading mechanisms. This work was supported in part by grants from DARPA and ONR.
CHAPTER 2
CASCADING FAILURES IN SPATIALLY-EMBEDDED DISTRIBUTED FLOW NETWORKS

2.1 Literature Review

The study of networks dates back centuries to the earliest known mathematical development of graph theory by Leonhard Euler in his 1736 paper on the "Seven Bridges of Königsberg" [13]. Since then, the breadth of the field has grown to encompass a variety of networks and models, in an attempt to capture the properties of real world complex systems. Of interest to this study are cascading failures. Numerous theoretical and computational studies have been conducted, and the understanding of cascade dynamics has improved over the decades yet is still inadequate. With technological advances motivating a rapid increase in social and physical connectivity, a strong grasp of the underlying dynamics of complex systems is crucial.

Our scientific expedition will explore network science research focused on the progression of cascades. One such work "Error and attack tolerance of complex networks" [14] discussed resilience as a function of network type. The degree distribution of a network is a distribution characterizing the number of edges attached to each node in the network. Some networks have characteristic degree distributions. The Erdős-Rényi model [15] describes a particular type of random graph with a binomial degree distribution, while the scale-free network [16] describes a graph with a power-law degree distribution. It has been found that the degree distribution of a network has a strong influence on its resilience when under attack. In the case of Erdős-Rényi graphs, random attacks on a subset of nodes have little variance in cascade severity. On the other hand, it has been found that scale-free networks

such as the World-Wide Web, social networks, social-media networks, and cell networks all exhibit high levels of resilience under random attacks or failures. The inhomogeneity of the degree distribution associated with such networks is crucial to this observed behavior. Scale-free networks have many low degree nodes whose failure is inconsequential to the stability of the network. To the contrary, there exist a small fraction of high-degree nodes in such networks whose extremely high level of connectivity translate to a topological disaster under failure or attack. For this reason, such networks are highly susceptible to targeted attacks, yet highly resilient to random failures. The Erdős-Rényi network on the other hand is not quite as susceptible to targeted attacks, but much less resilient under random attacks.

As interest in a fundamental understanding of such networks grew, the network science community took it upon themselves to develop new models. In one exemplary study ”A simple model of global cascades on random networks” [17] introduced the threshold model for modeling cascades in complex systems by modeling decision spread in a network through agent based modeling with agent opinions dependent upon those of their neighbors. The results found two regimes, one in which global cascades occurred often, and one in which they rarely occurred. The first regime is observed in low-degree networks, and power-law cascade size distributions are observed. It is found that high-degree nodes are more likely to spark large-scale cascades. The second regime occurs for highly connected networks where cascades are no longer dependent on network topology and are instead dependent upon the stability of individual nodes, thus avoiding power-law cascade size distributions. Instead a peculiar bimodal distribution of cascade sizes occurs. It was also found that networks with highly heterogeneous degree distributions were less vulnerable to cascading failures.

Motter et al. [18] was pivotal in the push to develop the study of cascading failures in distributed-flow networks. In his seminal work, he defined a cascade model in which flows were defined as the number of shortest paths that passed through a particular link or node in the network. The capacity of a node or link was then assumed to be the proportional to the flow (load) $L_j$ passing through that node, and the proportionality constant $\alpha$ was used to define the capacity:
\[ C_j = (1 + \alpha)L_j \]  

(2.1)

This model for assigning a capacity distribution to a distributed-flow network has been successfully recycled by many subsequent research publications. Motter et al. [18] focused on single-node failures in networks with various degree distributions. The goal was to identify links between the failure of an initial node in the network, and the level of damage induced in that network. Motter et al. studied scale-free networks, characterized by degree distributions with power laws

\[ P(k) \sim k^{-\gamma} \]  

(2.2)

with degree \( k \) and exponent \( \gamma \) and quantified the severity of the damage induced by a cascade by recording the size of the resultant giant component as a fraction of the original connected network size. The findings were that for networks with heterogeneous degree distributions, damage induced by the failure of nodes with high capacities was significantly greater than that induced by those with low capacities. For networks with homogenous degree distributions (as is the case with many spatially-embedded networks such as the power grid) the findings were inconclusive, and the severity of a cascade could not be predicted based on the characteristics of the node that induced the failure in the network.

Centola et al. [19] further studied cascade propagation, picking up on the study of cascades in random networks that was performed by Watts [17]. The main findings of Centola’s research were that random links between distant nodes would dramatically influence the progression of cascades, but the effect was highly network dependent. If the threshold model enables a single activated node to progress the cascade, it was found that such distant links could further facilitate cascades in the network. Conversely if a single active node is not able to progress a cascade, it was found that long range links would mitigate cascades. In similar research performed by Asztalos et. al. [20] it was found that cascading failures in spatially-embedded distributed flow networks are non-self-averaging. When a small fraction of long-range edges are added to these networks, self-averaging is reintroduced to
the system. These long-range links are preferable for predictability of cascading failure size in power grids. Contrary to the findings of Centola, Asztalos reported that long-range links increase the resilience of distributed flow networks; the key difference being that Centola focuses on the threshold model and not distributed flows. This suggests that network topology alone is not a sufficient predictor of the progression of cascading failures.

Many real-world networks behave similarly to the distributed flow model, and thus can all experience cascades. In a study of data packet transport on scale-free networks, Lee [21] modeled a distributed flow network in which the capacity of the nodes were assumed to be proportional to their initial loads with a proportionality constant of \((1 + \alpha)\) as suggested by Motter [18] in his 2002 seminal work. Lee found that for \(\alpha\) in a critical range, cascade size distributions generated by the system followed a power-law distribution. The observation of this critical phenomenon was not only identified through simulation. In a study of power-grid failure data, Hines [22] found that the distribution of cascading failure size in north american power failures also followed a power-law. More recent studies such as models including traffic flow [23], the power grid [18], [24], [25], and the internet [26], [27] have confirmed such results.

Network flows have been studied from a general perspective as so far discussed, but for particular applications it is necessary to assess whether these models reflect physical reality to the degree necessary for research purposes. Efforts have been put forth to understand how the modeling of power flows in non-linear AC and linearized DC models differ. Cetinay et. al. [28] recently concluded that the DC model generated results comparable to the AC model when evaluating load distribution in power systems. They studied multiple real-world networks in their stable state, as well as studying how well the DC approximation compared to the AC approximation under single edge failures. They also extended their work to study the difference in yield and line-vulnerability ratios of cascading failures on AC and DC power flow models. The general results of the findings are that the DC power flow equations provide similar results to the AC model when applied to small networks. As network size increases, the discrepancy between the AC and DC power flow models for cascading
failures increases.

When employing the steady-state approximations to power flow in real-world networks, transient effects associated with the sudden redistribution of load and change in power flow over a short time period are neglected. These are physical effects that will impact the progression of a cascade and can induce failures in nodes and edges that traditional AC or DC power flow models will neglect to address. Schäfer et. al. [29] have studied transient effects by analyzing the dynamics of topology changes in power systems by employing the swing equations in their full glory. The expectation is that loads can either exceed or not meet the load predicted by steady-state models. In the case loads are below steady-state predicted values, failures may be instantaneously mitigated. In the case where they exceed steady-state predicted values, failures will be more severe. The introduction of transient dynamics to a power flow model voids the traditional N-stable and \((N - 1)\) stable capacities, which is expected to increase the severity of cascades in the system. This is precisely what the models have found.

\[\text{2.2 Introduction}\]

In complex information or infrastructure networks even small localized disruptions can give rise to congestion that can trigger cascading failures (avalanches), a sequence of consecutive failures [30]. For example a single component failure in transportation networks can force a redistribution of traffic on the remaining portion of the network, which can cause subsequent congestion and failures. This phenomenon can be observed in various flow-driven systems such as infrastructure networks [1], [2], urban microgrids [3], commuter transportation and mobility networks [6], [4, 5], financial systems [7], and biological networks [8]. Among infrastructure networks a great interest is focused on the study of cascading failures occurring in electrical power grids [31], [22], [32], [33], [34], [35], [36]. Due to the latest technological advances, our modern society permanently relies on continuous and stable electricity provided by power grid systems. Any localized disruption can induce a cascading failure in the power grid, resulting in blackouts often over extended geographical regions, which can create life-threatening situations, and also cause
substantial financial losses. Cascading failures propagate at very high speeds, rendering real-time mitigations impractical in the event of a disruption.

Prior studies on cascading failures in power grids suggest that power grid blackouts follow a first-order phase transition [37]. Similarly, a recent study conducted on the US Western Interconnect power grid has revealed that the probability of cascading failures occurring, with respect to the value of the tolerance parameter, exhibits a bimodal nature, characteristic to first-order transitions [38]. These results indicate that a disruption in the system can either cause insignificant damage or trigger severe cascading failures. Another study conducted on scale-free networks has shown that within this phase transition region the number of failed nodes exhibits a power-law tail distribution [21]. Other studies have also reported a power-law behavior in the distribution of blackouts in power grids, phenomenon related to self-organized criticality [39]. Similarly, the size distribution of cascading failures in the North American power grid [32], as well as the size distribution of power blackouts for the Norwegian and North American power grids [40] also follow a power-law. Moreover, the power-law behavior has been detected in neuronal networks processing information, such as in the size distribution of neuronal avalanches [41].

In a more generalized context, power grid systems are spatially-constrained networks, characterized by short-range links. Asztalos, et al. [20] have shown that an extensively studied standard cascade mitigation strategy of preemptively disabling a fraction of underperforming nodes [42] is largely ineffective in spatially constrained networks. In addition, their study on the European power grid network [20] has revealed a lack of self-averaging in cascade processes, and showed that increasing the excess capacity does not reduce the severity of the cascade in a monotonic fashion. Therefore preventive measures, such as designing stable capacity allocation schema or identifying vulnerable regions are crucial to minimize the probability of severe failures.

Motivated by these prior results, we study a model of load-based cascading failures on spatial networks. In particular, we use the European power transmission network maintained and operated by the Union for the Co-ordination of Transmission of Electricity (UCTE), and study it as a resistor network carrying distributed
flow [43], [44]. We also employ Random Geometric Graphs (RGGs) [45], [46] for finite-size scaling analysis. Prior studies focused on resistor networks studied flow optimization, transport efficiency, and vulnerability in complex networks [44], [47], [48], [38]. We analyze the behavior of cascading failures in the UCTE network, and propose mitigation strategies to reduce the vulnerability of the system against random failures or targeted attacks. We find that mitigation against single-node failure can be effectively achieved, however as the complexity of disruption (number of failed nodes) increases, the predictability of the resulting damage becomes increasingly curtailed.

2.3 Methods

Below we describe the distributed flow model and cascade model that we use in our study.

2.3.1 Distributed Flow

We assume that the flow is distributed, directed and of unit size, associated with a source and sink, and flow through all possible paths between source and sink. We model the network as a simple random resistor network with unit conductances along the edges [48], [47]. In this model each node and edge is involved in transporting current from source to sink, therefore each link experiences a load which is the current along that edge. For a link connecting nodes $i$ and $j$ the load is calculated as $\ell_{ij} = I_{ij}^{st}$, and the load on an arbitrary node $i$ is the net current flowing through that node $\ell_i = I_i^{st}$. The two loads can be expressed as

$$I_i^{(st)} = \frac{1}{2} \sum_j |I_{ij}^{(st)}|$$  (2.3)

Next, we assume that all nodes are simultaneously sources and for each source we randomly choose a target from the remaining $N - 1$ nodes. Thus, we assume that unit current flows simultaneously between $N$ source/target pairs, and the load is defined as the superposition of all currents flowing through an arbitrary node. This is identical to the node current-flow betweenness [47], [49], [50], [51]:
\[ \ell_{ij} = \frac{1}{N-1} \sum_{s,t=1}^{N} |I_{ij}^{(st)}|, \ell_i = \frac{1}{N-1} \sum_{s,t=1}^{N} |I_{i}^{(st)}|. \quad (2.4) \]

In order to obtain the \( I_{ij}^{(st)} \) currents along the edges from one source/target pair, we use Kirchhoff’s law for each node \( i \) in the network and solve the system of linear equations:

\[ \sum_{j=1}^{N} A_{ij} (V_i - V_j) = I (\delta_{is} - \delta_{it}), \forall i = 1, \ldots, N. \quad (2.5) \]

Here, we assume that \( I \) units of current flow through the network from source \( s \) to target \( t \), and \( A_{ij} \) denotes the adjacency matrix of the network. This equation can be rewritten in terms of the weighted network Laplacian \( \mathcal{L} = \delta_{ij} k_i - A_{ij} \), where \( k_i = \sum_j A_{ij} \) is the degree of node \( i \). Thus, we can write Eq. 2.5 as \( \mathcal{L}V = \mathcal{I} \), where \( V \) is the unknown column voltage vector, and \( \mathcal{I} \) is the net current flowing into the network at node \( i \), and takes nonzero values only for the source and target nodes. Since the \( \mathcal{L} \) network Laplacian is singular, we find the pseudo-inverse Laplacian \( G = \mathcal{L}^{-1} \) using spectral decomposition \([44],[47],[52]\). Thus, by choosing as reference potential the mean voltage \([44], \hat{V}_i = V_i - \langle V \rangle \), where \( \langle V \rangle = (1/N) \sum_{j=1}^{N} V_j \) for each node \( i \) we obtain:

\[ \hat{V} = (GI)_i = \sum_{j=1}^{N} G_{ij} I (\delta_{js} - \delta_{jt}) = I (G_{is} - G_{it}) \quad (2.6) \]

Therefore, for \( I \) units of current and for a given source/target pair, the current flowing through edge \((i,j)\) can be written as

\[ I_{ij}^{(st)} = A_{ij} (V_i - V_j) = A_{ij} I (G_{is} - G_{it} - G_{js} + G_{jt}). \quad (2.7) \]

The above equation shows that current along an arbitrary edge is uniquely determined by network topology.

In modeling of the the electrical flows in the power grid a commonly used approach is the use of the DC power flow model \([30],[34],[37],[36],[53]\), where links, in addition to resistance also possess reactance. However, it has been shown in \([30]\)
that the equations for this DC model of power flow have identical mathematical structure to that of an analogous electrical circuit. In prior studies it has also been demonstrated that, despite neglecting the true AC nature of the power grid, inferences made by employing the DC power flow model can still generate useful results [37] but it has also been shown that the DC power flow model underestimates the severity of cascades [28], [29].

It is important to point out that our goal is to study the fundamental aspects of cascades on spatial networks carrying distributed flow, not designing strategies specifically tailored for electrical power transmission systems.

2.3.2 Cascade Model

We simulate the cascading failures in our networks using the model of Motter and Lai [18]. We assign each node a load-bearing capacity proportional to its initial state load in the form of \( C_i = (1 + \alpha) \ell_i^0 \), where \( C_i \) is the capacity of node \( i \), \( \ell_i^0 \) is its initial state load when the network is intact, and \( \alpha \) is a tolerance parameter. When a node fails, its load is redistributed among the surviving nodes. Nodes that after this redistribution are assigned a higher load than their capacity \( \ell_i > C_i \) also fail, resulting in further redistribution of load, and possible overload of other nodes. Such an avalanche of subsequent failures is called a cascading failure.

2.3.3 Empirical Network

Our work is centered on the study of the UCTE European power transmission network from year 2002 [54], [55]. The network comprises 18 European countries, contains \( N = 1254 \) nodes (buses) and \( E = 1812 \) edges (transmission lines). The average degree of the network is \( \langle k \rangle = 2.89 \).

2.3.4 Network Models

In addition to our study on the empirical UCTE power transmission network, we also test our methods on various types of artificial networks. Below, we briefly describe our approach in generating these synthetic network ensembles.

Random geometric graphs (RGG) We construct RGG graphs of size \( N \) in 2D by placing \( N \) nodes randomly in the unit square with open boundary conditions,
and connecting any pair of nodes if the Euclidean distance between them is less than the connection radius $R$ \cite{45}, \cite{46}. Based on $\langle k \rangle = \pi R^2 N$ formula, we control the average degree $\langle k \rangle$ of the graph by varying $R$.

**Scale-free (SF) networks** We construct scale-free networks \cite{16} of size $N$ by first generating a degree sequence from a prescribed power-law degree distribution $P(k) \sim k^{-\gamma}$ that yields a desired average degree $\langle k \rangle$. Next, we pass this degree sequence to the configuration model \cite{56} in order to obtain the scale-free network. Here, we consider the degree sequence as a list of the number of edge stubs (half-links) each node has, and in the configuration model we randomly choose two nodes with available edge stubs and connects them to form an edge. The process is repeated until all edge stubs are connected.

**Erdős-Rényi (ER) graphs** We construct ER graphs \cite{57} of size $N$ by connecting every pair of nodes with probability $p$, parameter used to control the average degree of the network using $\langle k \rangle = p(N - 1)$ formula.

### 2.3.5 Outlier Removal

To determine accurately which data points are outliers in order to remove them from our analysis, we calculate the prediction intervals and confidence intervals of our data. The confidence interval in Fig. 2.27 (blue) reveals the degree of uncertainty associated with a sample statistic, and is calculated from the observations. Prediction intervals or prediction bands Fig. 2.27 (green) establish the interval in which future observations will fall with a certain probability. For our correlation analysis we calculate in confidence interval and prediction bands based on our data, as seen in Fig. 2.27 insets. Next, we remove all data points that fall outside the prediction bands, and calculate the Pearson correlation coefficient.

### 2.4 Main Results

Our current work is centered on the study of spatial networks, namely the Union for the Co-ordination of Transmission of Electricity (UCTE) data set \cite{55} representing the power grid system of continental Europe in year 2002. The network comprises $N = 1254$ transmission stations and $E = 1812$ edges spanning 18
European countries. The network is disassortative with an assortativity coefficient of 0.1, with average degree $\langle k \rangle = 2.889$ and clustering coefficient of $C = 0.127$. We model the system as a random resistor network carrying distributed flow and employ a capacity-limited overload model [18] to simulate cascading failures in the network (see Methods). Note that despite the simplicity of this fundamental model for conserved flows (i.e. Kirchhoff’s and Ohm’s law in the resistor network), the underlying system of equations have identical structure to those of the DC power-flow approximation (the current and voltage corresponding to the power and phase, respectively) [3], [33], [58].

We find that the load is positively correlated with the degree, while the degree and load distributions span a relatively narrow range, yet a significant variance of loads can be observed even for small degree values. This characteristic suggests that the load bearing responsibility of a node cannot be assessed exclusively from its degree. Using the spatial information of the nodes and edges, we plot the link length distribution, and find that the majority of links span short distances with very few long range links constructed as part of the overall power grid designs. For the remainder of this article we use the terms removal of a node and attack on a node interchangeably to denote a node whose failure is used to initiate the cascade.

### 2.4.1 Stochastic Capacity Allocations

We start studying the behavior of cascading failures in the UCTE network by assigning to each node a uniform capacity proportional to its load $C_i = (1 + \alpha)l_i^0$, where $C_i$ is the total capacity of node $i$, $\alpha$ is a tolerance parameter [18], and $l_i^0$ is the initial state load of node $i$, when the network is intact. Further we will refer to $\Delta C_i = \alpha l_i^0$ as the excess capacity of node $i$.

In real-world scenarios, allocating additional protection against failures in interconnected systems comes at a cost, and assigning higher capacity to each node in order to mitigate cascading failures in the power grid can be a costly procedure. Therefore, we introduce a different approach for allocating the resources (capacities) in the power grid by using a stochastic random capacity allocation method, while preserving the same total cost in the system as for the previous uniform capacity al-
location case. The *mean* excess capacities assigned to the node $i$ are proportional to its normal equilibrium operational load $\overline{\Delta C_i} = \alpha l_i^o$. The particular values of the excess capacities, however, are drawn from a uniform distribution $\Delta C_i \in \alpha l_i^o[1 - \sigma, 1 + \sigma]$, with width $\sigma$ relative to the mean, such that $0 \leq \sigma \leq 1$, and subject to a fixed overall cost, $\sum_i \Delta C_i = \alpha \sum_i l_i^o$. In Fig. 2.1(b) we show that our fixed-cost random node-capacity assignment results in a significant and emergent broadening of the distribution of the size of surviving giant component $G$, by varying $\sigma$, the width of the search space. Hence, we can stochastically search for optimal excess capacity allocations resulting in maximum resilience (largest $G$). We also find that by choosing higher $\sigma$ values, we can further improve the protection against damage with no additional cost (albeit with a saturating effect). For baseline comparison we also plot the initial case when identical relative excess capacity is assigned to each node (black filled symbols). The results clearly demonstrate that the fixed-cost stochastic distribution of resources (capacities) allows for identifying particular realizations which provide superior protection against cascading failures in the power grid.

We study the cascading failure induced by the removal of a single (highest load) node from the network, and investigate the severity of the resulting damage, by calculating $G$, the size of the surviving giant component of the system. In Fig. 2.1 we observe cascades on the UCTE network triggered by the removal of a single (highest load) node. (a) The cascade size as a function of tolerance parameter for (a) uniform capacity allocation; (b) stochastic capacity allocation of varying $\sigma$ values: $\sigma = 0.25$ (green), $\sigma = 0.50$ (blue), and $\sigma = 1.00$ (red), with 100 simulations for each case. For comparison, the black connected data points show the performance of the uniform capacity allocation presented in (a). (c) Visualization of the damage caused in the UCTE power grid by the removal of the highest load node using the identical (uniform) capacity allocation vs. the best-case and worst-case scenario of the stochastic capacity allocations. (d) Correlation analysis of load/node degree vs. excess capacity for the best-case and worst-case scenario stochastic capacity allocations. In (a) we show that increasing $\alpha$ results in non-monotonic behavior of cascading failures. Higher capacity allocation (for example, an increase of $\alpha = 0.4$ to $\alpha = 0.45$) does not always reduce the severity of cascades, on the contrary, it
may induce larger damage in the system [20].

In Fig. 2.1(c) we illustrate for comparison the damage caused by the removal of the highest load node in case of uniform capacity allocation, the best-case scenario (the highest protection obtained from stochastic capacity allocation) and worst-case scenario (the lowest protection obtained from stochastic capacity allocation) when the tolerance is $\alpha = 0.45$ and the width of the stochastic search space is $\sigma = 1/2$.

Aiming to better understand the properties of the capacity allocations resulting in the highest protection vs. the lowest protection for a given $\alpha$ tolerance parameter, we study in Fig. 2.1(d) the correlation of the excess capacity with node degree and initial state load, but find little insight (based on traditional single-node structural or load-based characteristics) as to why a certain stochastic allocation of resources performs better than the others with respect to these node properties.

### 2.4.2 Sensitivity to Target Selection in Spatially-Localized Multi-Node Attacks

Previously, we triggered cascades by removing a single (highest load) node. In order to capture more realistic scenarios, we consider a geometrically concentrated region containing several nodes, and analyze how the selection of multiple spatially-clustered initiators influences the size of the induced damage. Specifically, we investigate the sensitivity of the cascades to small variations in the target set. We arbitrarily choose the center of our attacks to be in South Western Europe. A circular region of radius $1r$, $2r$, and $3r$ contains 9, 12, and 20 nodes, respectively, where $r \approx 60km$. We consider various attack realizations (i.e., selections of target set) in the $2r$ and $3r$ regions while keeping the total number of attacked nodes fixed to be 9.

We have seen in the single-node removal case a lack of correlation between the damage caused by a node, its degree, and its initial state load, respectively. Next, we analyze whether we can observe a correlation among these parameters in case of cascading failures triggered by multi-node attacks. In Fig. 2.2(a) we plot the size of the surviving giant component as a function of the sum of the initial state loads $\ell$ of the 9 initiator nodes removed from the $2r$ region. Once again, we
find that there is little or no correlation between traditional node characteristics (degree, load) and inflicted damage. Intuitively, one might expect to see a positive correlation between the load and damage, indicating that the failure of nodes with higher load would cause more severe damage. However, our results show that nodes with smaller load can cause severe damages, and nodes of similar load can induce minimal or no damage at all.

In Fig. 2.2 we present an analysis of node sensitivity in the UCTE network. (a) $G$ vs. $\sum_i e_i^{\text{initiator}}$. (b) $G$ vs. $\sum_i k_i^{\text{initiator}}$. (c) Contour plot of $2r$ region. (d) Contour plot of $3r$ region. (e) Visualization of variability for small changes in the target set for spatially-clustered attacks on the UCTE network. Case 1 and Case 2 visualize the avalanche of failed nodes (blue) triggered by the removal of two distinct sets of nine-spatially-localized-nodes (red) from the same $2r$ region, with $\alpha = 0.1$. Analyzing Fig. 2.2(b), we don’t observe any correlation between the damage induced by the nodes and the sum of their degrees $k$. Despite the lack of correlations between these quantities, it is interesting to observe a clear bimodal behavior in Fig. 2.2(a, b), with data points condensed around two regions: either causing severe damage of $G \in [0.3; 0.6]$ or inducing no cascading failure. Similar bimodal behavior has been reported for cascading failures in the US Western Interconnect (USWI) power grid [38].

Expanding our analysis of multi-node failures to larger attack regions ($2r$ and $3r$), we randomly select 9 nodes to be the initiators for one simulation, and perform 100 realizations for each region, and record the total degree and load of the initiators. In Fig. 2.2(c, d) we demonstrate how the cascading process varies among different node degrees and loads. The two-level distribution of $G$ implies that for the safety of the entire system, it is better to lower the degree and load in a potentially targeted region. In the smaller $2r$ region, the low damage and high damage separates clearly and seems to be of the same size. It is easier to mitigate the damage of cascades in a smaller region if the targeted region has a smaller total degree and load. However, the area of high damage is much larger than that of small damage in the case of $3r$, meaning most realizations suffer high damage. The border of these two areas is not smooth, indicating that it is more complicated to reduce the damage than
in the previous case. The results suggest that a larger region has a more complex topological structure, and that more variations of the initiators also increases the complexity of the resulting cascades.

For illustration, the nine nodes are attacked simultaneously and the resulting cascades for two different cases are shown in Fig. 2.2(e). The visualizations clearly imply that there is a very large variability in cascade size for small changes in a spatially-confined target set, depending on which 9 nodes (indicated by red) are selected out of 12 within the $2r$ region. For Case 1, the resulting cascade (indicated by blue) is relatively closely confined to the attack region, while for Case 2, the cascade impacts a major portion of the network, including regions far away from the attack center.

The progression of the cascade initiated by the removal of different node sets chosen randomly from a spatially-concentrated region, as well as the progression of the cascade initiated by the removal of different node sets chosen randomly when enlarging the spatially-concentrated region (increasing radius $r$) exhibits highly non-monotonic behavior.

2.4.3 $N$-Stable and $(N-1)$-Stable Capacity Allocation for the UCTE network

Next, we propose to study the UCTE network under two distinct system architectures based on power grid engineering methodology, namely the $N$-stable and $(N-1)$-stable configurations. The $N$-stable UCTE system represents the power grid network in its intact form with capacity allocation $C_i = (1 + \alpha)l_i^0$ [18]. Similarly, the $(N-1)$-stable system is designed such that it is stable against any single-node failure, when $(N-1)$ nodes are left in the network [30]. In order to attain this, we assign each node a capacity $C_i^{(N-1)}$, representing the minimum load capacity of node $i$ which guarantees that no subsequent overload failure occurs following any single-node failure in the system. Based on this we express the capacity of node $i$ as $C_i = (1 + \epsilon)C_i^{(N-1)}$, where $\epsilon$ is the relative tolerance. This method is used as an industry standard, and engineers commonly assign the relative tolerance values in the range of $\epsilon \in [0.1; 0.2]$. In our work we will further study the $(N-1)$-stable
using $\epsilon = 0.10$. In order to effectively compare the efficacy of the two network construction methods, we calculate the $\alpha$ value of the $N$-stable scenario that provides the same cost of protection as the $(N-1)$-stable scenario with $\epsilon = 0.10$. We find that $\alpha = 0.5927$ is the value for which the two systems use the same amount of resources, thus in the following analyses we will use $\alpha = 0.5927$ tolerance parameter for the $N$-stable case, and $\epsilon = 0.10$ relative tolerance for the $(N-1)$-stable case, unless otherwise stated.

Of great interest when studying attacks on networks is the role that spatial correlations, as well as the initial capacities on the nodes or edges of the intact network play in determining the severity of a cascade. Fig. 2.3(a, b) show the damage delivered by attacks on $N$-stable and $(N-1)$-stable networks, respectively. To initiate the cascade, nodes were either randomly chosen (with 5 realizations for each value of $n$), or removed in succession of distance from the center of the network (spatially correlated). The horizontal and vertical axes represent the number of removed nodes ($n$) triggering the cascade and the size of the surviving giant component ($G$) after the cascade, respectively. In both figures, the sum of the allocated capacities are equivalent, giving a fixed-cost comparison of the two system designs. It is immediately apparent that for small $n$ ($n < 100$) the $N$-stable and $(N-1)$-stable configurations are more stable against random failures, but are more vulnerable to spatially-localized attacks. As the number of targeted nodes becomes larger ($n \geq 100$), both systems become more vulnerable against random failures and more robust against localized attacks. What may be the most striking are the discontinuities in $G$ for the spatially-correlated scenario. As the radius of the attack increases, the severity of the damage slowly changes until certain critical radii are reached. There we witness abrupt changes in $G$, making the network more, or less robust depending on the location. This suggests that the severity of an attack on a network varies non-monotonically with the size of the attack. Smaller attacks may yield more damage and vice versa, similar to our previous findings. Also of importance is the fact that for smaller attacks, the spatially correlated attack is much more effective than the random attack. Possible reasoning for this observation is that a small random attack is unlikely to strike pivotal nodes, while a spatially correlated attack has a
much larger impact on one local region, disrupting the network more severely. The opposite is observed when the attack is large, and along similar lines of thought, it is unlikely that pivotal nodes in the network are clustered in one region. By dispersing the attack, the probability of hitting a higher number of such nodes increases.

Fig. 2.3(c) highlights the $1r$ (red circle) and $2r$ (blue circle) regions calculated from the geographic center of the UCTE network. For each $n$ there are 5 realizations of random attacks. The tolerance parameter of the $N$-stable system is $\alpha = 0.5927$, and for the $(N-1)$-stable $\epsilon = 0.1$. Visualization of $1r$ (red circle) and $2r$ (blue circle) regions used for spatially localized attacks in the UCTE network, where the distance is calculated from the geographic center of the network (red dot). In further spatially-localized attacks we will use the red and blue circled regions to analyze cascades induced by clustered node failures.

Next, we study the performance of the $N$-stable and $(N-1)$-stable UCTE network against various multi-node attacks. We remove 9 nodes from a $2r$ region, from the entire network, from the center, and finally, the nine-highest-load-nodes, and record the size of the surviving giant component $G$ for each scenario. For clarity, we sort the simulations in non-decreasing order of damage $G$ and present our results in Fig. 2.4. In Fig. 2.4(a), we again see the bimodal nature of spatially-localized attacks, either causing severe damage or not triggering cascading failures. Using the averaged values of the 500 simulations (solid lines), we can compare the performance of the two UCTE system designs, to conclude that for spatially-localized attacks in a $2r$ region the $N$-stable configuration outperforms the $(N-1)$-stable network. For the removal of nine-spatially-localized nodes we see that the $N$-stable scenario triggers cascading failures in less than 25% of simulations, whereas in the $(N-1)$-stable network, cascading failures are induced in approximately 50% of cases. Similarly, in the case of removing the nine-highest-load-nodes, we find that the $N$-stable configuration is almost 30% more robust than the $(N-1)$-stable network (see Fig. 2.4(d), dotted lines).

In Fig. 2.4(a) we see a nine-random-node removal from the $2r$ region; Fig. 2.4(b) nine-random-node removal from the entire network; Fig. 2.4(c) nine-center-node removal with stochastic capacity allocation; Fig. 2.4(d) nine-highest-load-node re-
moval with stochastic capacity allocation. Each removal scenario contains 500 repetitions on $N$-stable ($\alpha = 0.5927$) and on $(N-1)$-stable ($\epsilon = 0.1$) UCTE networks. For clarity purposes the sizes of the surviving giant component recorded at each trial are sorted in non-decreasing order. In Fig. 2.4(e) we see a comparison of stochastic search for optimal capacity allocation (red circle) with uniform capacity allocation (black line) for nine-center-node attacks on $N$-stable UCTE network with $\alpha = 0.5927$ and 500 trials; Fig. 2.4(f) comparison of stochastically optimized (red circle) and non-optimized uniform (black circle) capacity allocation against various tightly-clustered nine-node attacks with 1230 repetitions. The lines illustrate the average performance of each allocation. In Fig. 2.4(b) we can see that for nine-random-node removals (from the entire network) the robustness of both systems is improved, however in this case the $(N-1)$-stable configuration performs better, by inducing cascading failures in less than 20% of the simulations. Likewise, in the case of removing nine-center-nodes from the network, the $(N-1)$-stable configuration is more robust than its $N$-stable counterpart (see Fig. 2.4(c), dotted lines).

Using the stochastic capacity allocation method employed in the case of single-node removal, we study the damage caused by multi-node attacks when the $N$-stable and $(N-1)$-stable networks are assigned heterogeneous excess capacities. In the case of the $(N-1)$-stable configuration, the excess capacities are assigned from $\Delta C_i \in \epsilon C_i^{(N-1)}[1 - \sigma, 1 + \sigma]$, mean relative tolerance $\epsilon = 0.10$, search width $\sigma = 1$.

We find that in the case of nine-center-node removal (Fig. 2.4(c)), using stochastic capacity allocations, we can improve the performance of the $N$-stable configuration, while maintaining the same fixed-cost. It is important to notice that we can find optimal stochastic capacity allocations such that the nine-center-node removal does not induce cascading failures, maintaining the $N$-stable network intact. Also, as we have seen in the case of single-node failure, with stochastic capacity allocation we can also obtain allocation scenarios that offer higher protection than the uniform capacity allocation case. For the $(N-1)$-stable network, however, we cannot find stochastic allocation of resources that can outperform the uniform one. Moreover, we can see that each stochastic capacity allocation sample makes the system more vulnerable to failures. Since the $(N-1)$-stable configuration is already optimized for
any single-node failure, the stochastic capacity allocation perturbs this optimization, thus resulting in a more vulnerable system. In contrast, for the case of nine-highest-load-node removal, Fig. 2.4(d) shows that we can find random capacity allocations that improve the robustness of the \( (N-1) \)-stable system by almost 30\%. In addition, we can see that, on average, the \( (N-1) \)-stable configuration with random capacity assignment only slightly improves robustness of the \( (N-1) \)-stable system with uniform capacity allocation, however, it outperforms the \( N \)-stable network with random capacity assignment. Finally, overall, we can see that the \( N \)-stable network with uniform capacity allocation still remains significantly more robust than stochastic capacity allocations on both network constructs.

Lastly, we study the performance of stochastic capacity allocations optimized for a specific node removal in the event of a different attack scheme. Using the \( N \)-stable network configuration, we perform a stochastic search to obtain the optimal stochastic capacity allocation scenario for the nine-center-node attack, and present the results in Fig. 2.4(e). Next, using this optimal allocation, we test the robustness of the network against various tightly-clustered nine-node attacks. In Fig. 2.4(e, f) we show that similarly to the single-node removal case, we can successfully mitigate failures or attacks against "known" targets with the stochastic capacity allocation technique. While the optimized stochastic capacity allocation significantly outperforms the uniform one against the "known" nine-center-node attack, on average, both allocation schemes perform essentially the same against an arbitrary "unknown" nine-clustered-node attack Fig. 2.4(f). These results are also in agreement with our findings from the stochastic optimization analysis for single node attacks.

2.4.4 Multi-node Attack Strategies

Aiming to capture the consequences of various targeted attack strategies or random failures in power grids, we further expand our analysis. In Fig. 2.5(a) we observe the size of the surviving giant component \( G \) as a function of the total load of targeted nodes. The data points on the continuous lines represent the magnitude of the total load of the targeted nodes; the lines show the sizes of \( G \) when targeting
those nodes. Their color codes identify the used attack pattern: the four-highest-load-node removal (purple), the 4 nodes that removed together cause the highest damage, nodes selected by our greedy algorithm (green), the 4 nodes causing the highest damage when individually removed (blue). Fig. 2.5(b) compares the size of damage caused by various attack patterns by ranking $G$ in nondecreasing order. The figures contain 300 simulations for each attack scenario on the $N$-stable UCTE network with $\alpha = 0.5927$. Fig. 2.5(c) is a visualization of the nodes used in different attack patterns for triggering cascading failures in the UCTE network.

We study five different damage scenarios in the UCTE network that can truthfully reproduce possible attack schemes or breakdowns encountered in real-world situations. In the first method (random) we randomly select 4 nodes from the network and remove them simultaneously, thus depicting the outcomes of multi-node random failures or random attacks on the network. In the second method (clustered) we remove four-spatially-concentrated nodes, simulating cascading failure in case of an attack on a single large region. In the third method (4 max. individual damage) we select four nodes from the network that individually generate the most severe cascades, and remove them simultaneously. Next, the 4 max. individual load method reflects the scenario of simultaneously attacking the highest load nodes in the network. We can observe a fundamental non-monotonic feature of the cascading overload failure process: attacking only the (single) largest-damage inducing node in the network results in a smaller surviving giant component $G$ (and a larger overall damage) than the simultaneous attack of the 4 max. individual load nodes Fig. 2.5(a).

In the final method (greedy selection strategy) we select the 4 nodes that trigger the largest cascading failures when removed simultaneously. In order to find these nodes, first we identify the single most damaging node by scanning all $N$ single-node failures. Then we determine the second node that causes the highest damage by scanning all remaining $N-1$ nodes on top of the failure caused by the first identified node, and continue in this manner until we have identified a set of the 4 most damaging nodes. The comparison of the effects of these five cascade triggering methods is captured in Fig. 2.5(a). The data points comprise 300 runs for each
scenario on the $N$-stable UCTE network, with tolerance parameter $\alpha = 0.5927$. We find that the random and clustered attacks cause similar damage in the network, and in most cases the system remains intact, without triggering a cascading failure. In Fig. 2.5(b) we rank the size of the damage ($G$) in non-decreasing order to create a more visually compelling comparison of the impact of the damages induced by the different attack scenarios. This figure shows that among 300 simulated random and spatially clustered attacks, only about 50 (approx. 15%) cases induce damage in the system. However, attacks by the three other selection strategies trigger more severe cascading failures in the power grid. Moreover, the greedy method, where we choose the 4 most damaging nodes, triggers the strongest cascading failure, under which the surviving giant component is nearly 10% of the initial network. This means that removing only 4 nodes can induce an almost complete system failure, a magnitude of damage that no other method can achieve. On the other hand, the random node failures or spatially-clustered attacks have minor effects on the network, causing the smallest damage in the system compared to the other attack strategies.

2.4.5 Phase Transitions in Cascading Failures

In Fig. 2.6(a) we have a four-center-node removal in the $N$-stable UCTE network. Fig. 2.6(b) shows a nine-center-node removal in $(N-1)$-stable UCTE network. Fig. 2.6(c) shows a four-center-node removal in $N$-stable UCTE network. Fig. 2.6(d) shows a four-center-node removal in $(N-1)$-stable UCTE network. The pink highlighted areas depict the region before the transition, after which the network becomes fully protected against failures. For comparison with synthetic networks we analyze phase transition in RGGs when cascades are triggered by the removal of the highest load node Fig. 2.6(e) with 3 different RGG network samples of identical size $N = 1000$ and average degree $\langle k \rangle = 10$; Fig. 2.6(f) with 4 realizations of RGG of same average degree $\langle k \rangle = 10$, but different system sizes. The inset shows the second largest component ($G_2$) sizes for the corresponding networks.

Asztalos et al. [20] have reported that by increasing the tolerance parameter in the system, one can observe a non-monotonic behavior in the size of the surviving giant component. Likewise, as seen in Fig. 2.6(a-d), we show that in the $N$-stable
and \((N-1)\)-stable UCTE network configurations, by varying the value of \(\alpha\) and \(\epsilon\) tolerance, respectively, we can also notice a similar, non-monotonic trend for various spatially localized attacks. The encircled highlighted regions depict the tolerance values for which the system becomes vulnerable to large-scale cascading failures. By increasing the protection beyond these values, in both \(N\)-stable and \((N-1)\)-stable cases, we can determine a certain tolerance value, where the system undergoes a phase transition, after which the network almost completely survives an attack. The \((N-1)\)-stable network reaches full protection at a much smaller tolerance value, due to the fact that it is already designed to be protected against any single-node failure, deeming it with a higher base capacity allocation. It should be noted that the sum of the capacities afforded to both the \((N)\) and \((N-1)\)-stable networks are nearly identical.

In addition, aiming to provide a generalized behavior in spatial networks of the observed transition property, we study the phase transition of cascading failures in RGGs, and find that despite using a different removal strategy, single (highest load) node removal, we obtain similar bimodal behavior in the size of induced damages. However, as Fig. 2.6(e) indicates, we cannot assess a universal tolerance value where the phase transition occurs, because different spatial network instances despite having identical network properties (system size, average degree), present a realization-specific different non-monotonic increase with critical points at different tolerance values. Moreover, we show in Fig. 2.6(f) that by increasing the system size, we can see the same non-monotonic behavior in the severity of cascades, with a phase transition occurring at different critical \(\alpha\) values. In addition, the inset of Fig. 2.6(f) illustrates the size of the second largest component \(G_2\) for the corresponding networks, revealing a similar non-monotonic behavior. Tracing the behavior of the second largest component can be useful to identify changes in the network’s stability and robustness and the onset of a possible phase transition [57], [59]. Once again these results indicate the complex nature of spatial networks, and the difficulty in predicting the behavior of cascading failures in such systems.
2.4.6 Cascade-size Distribution Analysis

Next, we study the cascade size distributions in the phase transition regimes, where, according to prior studies, such distributions are characterized by power-law tails. We quantify the cascade size $S$ as the number of nodes that fail during a cascading process. For comparison, in Fig. 2.7 we plot the cascade distributions both as $G$ and $S$. Since $S$ is the number of failed nodes, and $G$ is the size of the surviving giant component, $S \neq N - G$. In Fig. 2.7(a) we show a power-law fit (red line) of four-clustered-node removals (black dots) with $\alpha = 0.6$. Fig. 2.7(b) shows a power-law fit (red line) of four-random-node removals (black dots) with the same $\alpha$ value. Fig. 2.7(c) shows a power-law fit of four-clustered-node removals (black dots) with $\alpha = 0.8$. Finally Fig. 2.7(d) shows a power-law fit (red line) of four-random-node removals (black dots) with $\alpha = 0.8$; small event regime $1 \leq S \leq 200$, large event regime: $201 \leq S \leq 300$. Fig. 2.7(e) shows a power-law trend of cascade size distributions for random single-node removal in RGGs of different systems sizes and $\langle k \rangle = 10$ for $\alpha = 0.45$ and (f) $\alpha = 0.50$.

Given the strong linear correlation between $G$ and $S$, both variables can be used interchangeably to measure cascade severity. The cumulative cascade size distributions exhibit a power-law tail $P_{>}(S) \sim \frac{1}{S^\gamma}$ with exponent $\gamma$, and cascade size distributions can be found as $p(S) \sim \frac{1}{S^{\gamma+1}}$. We focus on cascading failures on the $N$-stable configuration triggered by spatially-clustered sets of 4 nodes or random sets of 4 nodes distributed throughout the network for an $\alpha$ value fixed within the phase transition region, and record the distribution of cascade sizes as the fraction of blackouts of size $S$ or larger. In Fig. 2.7(a) and Fig. 2.7(b) we show that both triggering methods generate power-law tail distributions. We also find that increasing the $\alpha$ tolerance parameter from $\alpha = 0.60$ to $\alpha = 0.80$ the cascade size distribution becomes more abrupt, producing a higher power-law exponent. This observation can be explained intuitively; by increasing the tolerance parameter, we increase the protection in the system, and reduce the number of large cascades, thus increasing the number of small failures. As seen in these figures, for $\alpha = 0.60$ both cascade size distributions triggered by clustered sets of 4 nodes and random sets of 4 nodes exhibit a dual plateau. Thus, in Fig. 2.7(a, b) we analyzed these as...
two separate event regimes: the small event regime, where the size of the cascading failures is small \((1 \leq S \leq 200)\), and the large event regime, where the resulted failures are large \((201 \leq S)\). We can see that both triggering methods produce similar cascade size distributions, with power-law exponents of \(\gamma \approx 0.3\) in the small event regime, and \(\gamma \approx 2.7\) in the large event regime. Our results are in agreement with previous work [40], where the probability density of conductance changes also follow a power-law, with two different regimes, reported both for synthetic networks and the Norway power grid system. Moreover, the values of the reported power-law exponents in the two distinct regimes are close to the values observed in our work on the UCTE network. We employ statistical testing methods to assess the validity of power-law fitting, and describe the used methodology briefly in the Methods section and more specifically discuss the topic in the Further findings section.

Our results also indicate that a power-law tail of the cascade-size distribution only emerges when the values of \(\alpha\) and \(\epsilon\) tolerance parameters are within the “critical region” (close enough to an underlying phase transition), in agreement with the observation reported in [21]. Further, in Fig. 2.7(e, f), we test our finding on random geometric graphs (RGGs), and observe a similar power-law trend in the cascade-size distribution when we trigger the cascade by the removal of a single (highest load) node. For RGGs, however, we also have the ability to carry out a detailed finite-size analysis for increasing network sizes. Our results show that within the critical region, but below \(\alpha_c\), the power laws exhibit a \textit{system-size-independent} cut-off Fig. 2.7(e). On the other hand, at around the critical value of \(\alpha\), there appears to be no cut-off, and range of power-law scaling is progressively pushed out for larger and larger system sizes Fig. 2.7(f). Also in RGGs, as we move away from the phase transition region, the power-law characteristic vanishes. At \((\alpha = 0.45)\) and near \((\alpha = 0.50)\) critical values we find similar power-law trend in RGGs of various system sizes \((N=1000, \ N=4000, \ N=10000)\). The fitted power-laws for each system size are presented in the further findings section.
2.4.7 Predicting the Severity of Cascading Failures

So far we have analyzed mitigation strategies and the behavior of cascading failures triggered by various strategies of node removals. Here, we study the predictability of damage caused by the failure of a set of nodes $G^{total}$, given the sum of damages caused by each individual node failure, $\sum G_i^{initiator}$ which are the sums of the surviving giant components (in the further findings section we also present this analysis for $S$ avalanche sizes). Using various numbers of initiator nodes and different removal strategies, we show in Fig. 2.8(e, f) that there is a strong linear correlation between the variables. This indicates that given a set of node failures, and knowing the damage induced solely by the failure of each individual node, we can effectively predict the damage induced in the event of a multi-node failure. The insets show results for 300 samples, however, based on the confidence intervals of the data, we have removed a small fraction of outlier nodes. A detailed description of the strategy used to identify these outliers is presented in the further findings section. Additionally, we present these correlations for different sizes of multi-node failures ranging from 2 to 9 simultaneously failed nodes, and show that as we increase the number of simultaneously failed nodes, the correlation significantly drops. This finding once again suggests that accurate estimation of damage is harder to attain as the complexity of the cascade (number of triggering nodes) increases.

To understand the mechanism responsible for the correlation between single-node and multiple node attacks, we investigate various characteristics of the cascading failures in question. We find in Fig. 2.8(g, h) that the sum of individual node failures $\sum G_i^{initiator}$ and the failure of the individual node that triggers the largest damage $\min G_i^{initiator}$ (lower G represents higher damage) correlate equally with a multi-node failure $G^{All\; initiators}$. This suggests that for multi-node failure scenarios, the node which individually inflicts the highest level of damage on the network is responsible for the progression of the multi-node cascade, which implies the existence of dominating modes of cascading failures. For most scenarios, the remaining nodes have little to no effect on the progression of the cascade. However, when multiple critical nodes, (nodes that individually inflict the highest damage) are triggered simultaneously, we find a poor correlation between individual and multi-node
failures.

Finally, in order to study whether there is a correlation between initial network characteristics and cascade severity, we run extensive numerical simulations of individual node removals for varying $\alpha$ values. The correlation over all attacks for various alpha values are presented in the further findings. We observe that as the tolerance of the network is increased, the system remains unaffected by a higher percentage of the attacks. A correlation over various alpha values would indicate that the network topology is responsible for the cascade progression. We find a weak, but existent correlation suggesting that while topology is important, the cascade progression is also highly dependent on tolerance value. This finding is intuitive, since the network topology is continually disintegrated throughout the cascading failure process.

2.5 Further Findings

2.5.1 UCTE Network Properties

The Union for the Co-ordination of Transmission of Electricity (UCTE) data set [55] represents the power grid system of continental Europe during 2002. The network comprises $N = 1254$ transmission stations and $E = 1812$ edges spanning 18 European countries. The network is disassortative with an assortativity coefficient of 0.1, with average degree $\langle k \rangle = 2.889$ and clustering coefficient of $C = 0.127$. We model the system as a random resistor network carrying distributed flow and employ a capacity-limited overload model [18] to simulate cascading failures in the network. Note that despite the simplicity of this fundamental model for conserved flows (i.e., Kirchhoff’s and Ohm’s law in the resistor network), the underlying system of equations have identical structure to those of the DC power-flow approximation (the current and voltage corresponding to the power and phase, respectively) [3], [33], [58].

We show in Fig. 2.9 that the load is positively correlated with the degree, while the degree and load distributions span a relatively narrow range, yet a significant variance of loads can be observed even for small degree values. This characteristic suggests that the load bearing responsibility of a node cannot be assessed exclusively
from its degree. Using the spatial information of the nodes and edges, we plot the link length distribution Fig. 2.9(c), and find that the majority of links span short distances with very few long range links constructed as part of the overall power grid designs. For the remainder of this article we use removal of a node, and attack on a node interchangeably to denote a node whose failure is used to initiate the cascade.

We define the sensitivity of a node as the size of the surviving giant component resulting from the failure of that individual node. In Fig. 2.10 we visualize the sensitivity of each node in the UCTE network. Red indicates highly sensitive nodes, their individual removal leading to severe system damage. We find that the failure of leaf nodes has minimal impact on the network. Otherwise, correlations between damage size and topological characteristics of a node are difficult to detect visually. Yet it is apparent that nodes found in the extremities of the network (locations of Italy, Spain, France, Portugal) do not impart large cascades on the network through single node failures.

2.5.2 Analysis of Optimal Stochastic Capacity Allocation Characteristics

Random capacity assignment from heterogeneous distributions have shown that we can stochastically find allocations that mitigate cascading failures, but can also obtain realizations that lead to higher damage in the system as opposed to the uniform capacity allocation. We choose two random capacity allocation scenarios. One in which the robustness of the systems was most improved, and one in which the robustness of the system was most diminished. We aim to analyze whether increasing the capacity allocation to a certain subset of nodes helps improve the robustness of the system. We analyze the degree of a node vs. the amount of excess capacity allocated to that particular node in hopes of finding a trend common to the best stochastic capacity allocations, and conversely a trend common to the worst stochastic capacity allocations. We analyze the correlation between node properties and excess capacity assignment for "best/worst-case" scenarios in Figs. 2.11-2.14. The analyzed characteristics are node degree, load, a combination
of both properties, and the identity of the node. We are unsuccessful in finding an apparent difference between these allocations that would explain the differing robustness given the capacity allocations.

In figs. 2.15(a-b) we observe node sensitivity for single-node failures. The red line highlights the averaged value of the data points. Figs. 2.15(c-d) show node sensitivity for single-node failure rank ordered by the size of surviving giant component. Figs. 2.15(e-f) show histograms visualizing the distribution of the size of surviving giant component for single-node failures. We observe a bimodal distribution of cascade sizes as originally show by Watts in his model for flow-based networks [17]. In the UCTE network we conjecture that the bimodal distribution is given rise by the topology of the network. A central subset of the network may be particularly vulnerable to cascading failures. The failure of this subset of the network is a binary occurrence. When it fails, the cascade yields giant component sizes below $G \approx 0.6$, otherwise the cascade is fairly weak as seen in Figs. 2.15(e-f).

2.5.3 Non-monotonic Behavior Under Spatially-Correlated Attacks

In Fig. 2.16 we trigger cascades by removing the same set of 9 nodes (red) from a localized region near Barcelona in the UCTE network for two different tolerance ($\alpha$) values. We show that a smaller tolerance parameter leads to a smaller damage (left), whereas a higher tolerance parameter of $\alpha = 0.15$ (right) causes a larger cascading failure. This result highlights the importance of understanding the governing dynamics behind cascade progression, because as show providing a greater amount of resources to the system can decrease its robustness. Conversely, providing less resources in a scientifically informed fashion can improve the robustness of the system. The justification for such behavior can be attributed to fuse nodes. When allocated with a higher tolerance, the individual nodes of the UCTE network are safeguarded from failure. This is generally beneficial unless the node in question is a fuse node. Fuse nodes have the peculiar property of hindering the progression of a cascade through their failure. They prevent load overflows from accessing highly-sensitive regions of the network that would otherwise promote devastating cascade dynamics. For this reason paying less in resources can improve robustness, and paying more in
resources can reduce robustness in distributed flow networks.

2.5.4 Node Sensitivity in Random Geometric Graphs (RGGs) and Scale-Free Networks

So far we have studied the node sensitivity of the UCTE network. Next, we generate artificial networks to analyze and compare the sensitivity of nodes under different topological constraints. In Fig. 2.17 the subfigures plot the size of the surviving giant component (in case the cascade is triggered by the removal of a single-node) as a function of node load in (a) scale-free (SF) network with system size $N = 1000$ and $\langle k \rangle = 3$, (b) UCTE network, (c) scale-free (SF) network with system size $N = 1000$ and $\langle k \rangle = 10$; (d) random geometric graph (RGG) with system size $N = 1000$ and $\langle k \rangle = 10$. Each network is constructed with $\alpha = 0.45$ tolerance parameter. We observe that RGGs, similar to the UCTE network show no correlation between sensitivity and node degree, whereas scale-free (SF) networks exhibit a correlation between node degree and sensitivity. Similar behavior can be found in low $\langle k \rangle = 3$ average degree as well as high $\langle k \rangle = 10$ average degree RGG and SF systems.

To understand why a correlation between initial load and cascade size is only found in scale-free networks, we must consider the topology of such networks. In these networks there exist many low degree nodes and a smaller number of higher degree nodes. The function of highly connected nodes is to keep the network connected. Therefore when a high-degree node is attacked, the network is likely to immediately disintegrate into disconnected components. Given our measure of cascade size as the magnitude of the largest connected component in the resulting network, it is apparent why such topologies suffer from attacks on high-degree nodes. In other words, the heterogeneity of the degree distribution and the hierarchical structure of scale-free networks motivate the relation between node degree and cascade size. In spatially embedded networks such as the random geometric graph and the UCTE network, the topology favors local connectivity, and a failure in one region generally effects the local neighboring area during one cycle of the cascade. In addition, the probability of network segmentation due to a single node failure in a network
with a homogeneous degree distribution is very low, again due to the highly local connectivity of such networks.

We analyze the severity of cascading failures in RGG networks of various system sizes and varying $\alpha$ values in Fig. 2.18. Cascades are triggered by the removal of the highest load node on RGG networks of size (a) $N = 1000$, (b) $N = 2000$, (c) $N = 10000$, with 3 different realizations for each system size. (d) Analysis of non-monotonic behavior scaling with system size. Simulations are performed on synthetic random geometric graphs (RGGs) of average degree $\langle k \rangle = 10$ and various $N$ system sizes. It is immediately apparent that there exists a phase transition over tolerance ($\alpha$) above which the RGG network is minimally affected by attacks on the highest load node. There is no reason to believe that the phase transition would diminish as the system size grows. Contrarily, the emergent statistical behavior observed should only be fortified as the network size increases. Non-monotonic behavior is visible for various system sizes, and it can be seen that the non-monotonic behavior of these systems decreases as a function of size. As the system size increases, the behavior of the system becomes more dependent on the aggregate behavior of the full set of nodes, and less on particular nodes. This reduction of influence from individual nodes, and greater dependence on aggregate system behavior can be expected to increase with network size, with non-monotonicity disappearing for infinitely large networks.

2.5.5 Failure Response in $N$-Stable and $(N-1)$-Stable Networks
Figure 2.1: Cascades on the UCTE network triggered by the removal of a single (highest load) node. (a) The cascade size as a function of tolerance parameter for (a) uniform capacity allocation; (b) stochastic capacity allocation of varying $\sigma$ values: $\sigma = 0.25$ (green), $\sigma = 0.50$ (blue), and $\sigma = 1.00$ (red), with 100 simulations for each case. For comparison, the black connected data points show the performance of the uniform capacity allocation presented in (a). (c) Visualization of the damage caused in the UCTE power grid by the removal of the highest load node using the identical (uniform) capacity allocation vs. the best-case and worst-case scenario of the stochastic capacity allocations. (d) Correlation analysis of load/node degree vs. excess capacity for the best-case and worst-case scenario stochastic capacity allocations.
Figure 2.2: Node sensitivity in the UCTE network. (a) $G$ vs. $\sum_i l_i^{\text{initiator}}$ (b) $G$ vs. $\sum_i k_i^{\text{initiator}}$ (c) Contour plot of $2r$ region (d) Contour plot of $3r$ region (e) Visualization of variability for small changes in the target set for spatially-clustered attacks on the UCTE network. Case 1 and Case 2 visualize the avalanche of failed nodes (blue) triggered by the removal of two distinct sets of nine-spatially-localized-nodes (red) from the same $2r$ region, with $\alpha = 0.1$. 

\[37\]
Figure 2.3: Spatially-concentrated and distributed (random) attacks in $N$-stable and $(N-1)$-stable UCTE networks. For each $n$ there are 5 realizations of random attacks. The tolerance parameter of the $N$-stable system is $\alpha = 0.5927$, and for the $(N-1)$-stable $\epsilon = 0.1$. (c) Visualization of $1r$ (red circle) and $2r$ (blue circle) regions used for spatially localized attacks in the UCTE network, where the distance is calculated from the geographic center of the network (red dot).
Figure 2.4: Multi-node attacks on $N$-stable and $(N-1)$-stable UCTE networks. (a) nine-random-node removal from the $2r$ region; (b) nine-random-node removal from the entire network; (c) nine-center-node removal with stochastic capacity allocation; (d) nine-highest-load-node removal with stochastic capacity allocation. Each scenario contains 500 repetitions on the $N$-stable ($\alpha = 0.5927$) and $(N-1)$-stable ($\epsilon = 0.1$) UCTE network. (e) Comparison of stochastic search for optimal capacity allocation (red circle) with uniform capacity allocation (black line) for nine-center-node attacks on the $N$-stable UCTE network with $\alpha = 0.5927$ over 500 trials. (f) Comparison of stochastically optimized (red circle) and non-optimized uniform (black circle) capacity allocations against various tightly-clustered nine-node attacks with 1230 repetitions.
Figure 2.5: Severe attack patterns in the $N$-stable UCTE network. (a) Size of the surviving giant component $G$ as a function of the total load of targeted nodes. The data points on the continuous lines represent the sizes of the total load of the targeted nodes; the lines show the sizes of $G$ when targeting those nodes. Their color codes identify the attack pattern used: the four-highest-load-node removal (purple), the single node that individually causes the greatest damage, nodes selected by our greedy algorithm (green), the 4 nodes causing the highest damage when individually removed (blue). (b) Comparison of the size of damage caused by various attack patterns by ranking $G$ in nondecreasing order. 300 simulations for each attack scenario on the $N$-stable UCTE network with $\alpha = 0.5927$. (c) Visualization on the UCTE network of the nodes used in the different attack patterns for triggering the cascading failures.
Figure 2.6: Phase transitions with increasing protection in UCTE and RGG networks. (a) four-center-node removal in $N$-stable UCTE network. (b) nine-center-node removal in $(N-1)$-stable UCTE network. (c) four-center-node removal in $N$-stable UCTE network. (d) four-center-node removal in $(N-1)$-stable UCTE network. (e) 3 different RGG networks of identical size $N = 1000$ and average degree $\langle k \rangle = 10$; (f) 4 realizations of RGGs $\langle k \rangle = 10$, of different system sizes. The inset shows the second largest component ($G_2$) sizes for the corresponding networks.
Figure 2.7: Power-law tail of cascade size distributions in the phase transition regime. (a) Power-law fit (red line) of four-clustered-node removals (black dots) with $\alpha = 0.6$. (b) Power-law fit (red line) of four-random-node removals (black dots) with $\alpha = 0.6$. (c) Power-law fit of four-clustered-node removals (black dots) with $\alpha = 0.8$. (d) Power-law fit (red line) of four-random-node removals (black dots) with $\alpha = 0.8$. Small event regime $1 \leq S \leq 200$, large event regime: $201 \leq S \leq 300$ (e) Power-law trend of cascade size distributions for random single-node removal in RGGs of different systems sizes and $\langle k \rangle = 10$ for $\alpha = 0.45$ and (f) $\alpha = 0.50$. 
Figure 2.8: Correlation analysis of failures triggered by the failure of 4 nodes on the UCTE network. $\alpha = 0.5927$ (relative tolerance); 300 repetitions of four-random-node failures from the entire network.
Figure 2.9: Properties of the UCTE network. (a) Node degree distribution; (b) correlation between node degree and node load; (c) histogram of link length distribution.
Figure 2.10: Node sensitivity of single-node removal in the UCTE network. The color hue indicates the size of damage (surviving giant component) when that single node fails.
Figure 2.11: Comparison of best-case and worst-case excess capacity allocations as a function of node degree in the UCTE network. $\Delta C_i$ vs. $K_i$ for (a) Best-case for $\alpha = 0.40$, (b) worst-case for $\alpha = 0.40$, (c) best-case for $\alpha = 0.45$, (d) worst-case for $\alpha = 0.45$. 
Figure 2.12: Comparison of best-case and worst-case excess capacity allocations as a function of initial state node load in the UCTE network. $\Delta C_i$ vs. $\ell_i$ for (a) Best-case for $\alpha = 0.40$, (b) worst-case for $\alpha = 0.40$, (c) best-case for $\alpha = 0.45$, (d) worst-case for $\alpha = 0.45$. 
Figure 2.13: Comparison of best-case and worst-case excess capacity allocations in the UCTE network. (a) Comparison of excess capacity, normalized by initial state load, as a function of node degree for $\alpha = 0.40$ and (b) $\alpha = 0.45$. (c) Comparison of excess capacity, normalized by initial state load, as a function of initial state node load for $\alpha = 0.40$ and (d) $\alpha = 0.45$. 
Figure 2.14: Comparison of best-case and worst-case excess capacity allocations by node ID in the UCTE network. (a) Best-case for $\alpha = 0.40$, (b) worst-case for $\alpha = 0.40$, (c) best-case for $\alpha = 0.45$, (d) worst-case for $\alpha = 0.45$. 
Figure 2.15: Comparison of UCTE network with uniform capacity allocation (left) and UCTE network with stochastic best-case capacity allocation (right). (a-b) Node sensitivity for single node failure. The red line highlights the averaged value of the data points. (c-d) Node sensitivity for single node failure rank ordered by the size of surviving giant component. (e-f) Histograms visualizing the distribution of the size of surviving giant component for single node failures.
Figure 2.16: Non-monotonic behavior in spatially-correlated attacks in the UCTE network vs the tolerance. We trigger the cascades by removing the same set of 9 nodes (red) from the $1r$ region in the UCTE network for two different tolerance ($\alpha$) values. We show that a smaller tolerance parameter leads to a smaller damage (left), whereas a higher tolerance parameter of $\alpha = 0.15$ (right) causes a larger cascading failure. This result suggests the presence of fuse nodes, which can prevent the spreading of cascades in case they fail due to a lower capacity allocation.
Figure 2.17: Node sensitivity analysis for single node removal. The subfigures plot the size of the surviving giant component (in case the cascade is triggered by the removal of a single node) as a function of node load in (a) scale-free (SF) network with system size $N = 1000$ and $\langle k \rangle = 3$, (b) UCTE network, (c) scale-free (SF) network with system size $N = 1000$ and $\langle k \rangle = 10$; (d) RGG with system size $N = 1000$ and $\langle k \rangle = 10$. Each network is constructed with $\alpha = 0.45$ tolerance parameter.
Figure 2.18: Sample-to-sample fluctuation and finite-size behavior of cascading failures on RGGs. Cascades triggered by the removal of the highest load node on RGG networks of size (a) $N = 1000$, (b) $N = 2000$, (c) $N = 10000$, with 3 different realizations for each system size. (d) Analysis of non-monotonic behavior scaling with system size. Simulations performed on synthetic random geometric graphs (RGGs) of average degree $\langle k \rangle = 10$ and various $N$ system sizes.
Figure 2.19: Required capacity comparison for $N$-stable and $(N-1)$-stable UCTE network constructions.

In Fig. 2.19 we analyze the required capacity allocations for each node in the case of $N$-stable UCTE in comparison with the $(N-1)$-stable scenario. The y-axis represents the minimum capacity required for the system to meet $N$ or $N-1$ stability requirements. The $(N-1)$-stable capacity set requires an additional 45% capacity allocation over that required by the $(N)$-stable set over the whole network.

In Fig. 2.20 we compare cascades induced by 9 random nodes from a circular region of $2r$. All cascade simulations are at a fixed cost of resources to the full system. In (a-d) we observe that the $(N-1)$-stable set allows for more devastating cascades of size $G \approx 0.2$ where the minim cutoff for the $(N)$-stable set is above 0.3. We observe a strict bimodal distribution for both scenarios. From (e, f) it is apparent that the $(N)$-stable set of capacities provides much higher resilience to the network. The fraction of scenarios experiencing devastating cascades is above 80% for the $(N-1)$-stable capacity set and approximately 60% for the $(N)$-stable set.

In Fig. 2.21 we analyze cascading failures in the $N$-stable and $(N-1)$-stable UCTE networks by removing multiple nodes, and identifying "fuse" nodes; nodes whose failure prevents the transport of load to sensitive regions which induce high levels of damage in the system. We attack the nodes closest to the center of the network as labelled on the x-axis of the plot. These are spatially-correlated attacks applied to a confined circular region growing with the number of attacked nodes. As shown, there is a discontinuity in the level of damage induced for the $N$-stable
Figure 2.20: Nine-random-node removals from $2r$ region for (a) $N$-stable and (b) $(N-1)$-stable UCTE network.

capacity set when the 74th node is included in the attack. In the $N$-stable capacity set, the failure of this node exaggerates the damage experienced by the system. Peculiarly, while in the $N$-1-stable system, we see that the failure of the same node improves the robustness of the network against the same attack. This elucidates the importance that the capacity distribution has on the progression of cascades, as
Figure 2.21: Stability of $N$-stable and $(N-1)$-stable UCTE networks against multi-node attacks. The two blue nodes on the UCTE network visualization depict critical nodes (fuses) that increase the damage in the system in the case where they survive.

the redistribution of loads follows a greatly different landscape for different capacity distributions. The node can be said to be critical, yet the criticality of the node can be either to the benefit or the detriment of the network. We see very similar behavior for the inclusion of the 133rd node in a concentric attack. In this case, the $N$-stable system experiences a slight improvement in robustness while the $N-1$-stable experiences a reduction. This suggests that the effect of critical nodes varies as different capacity allocations are implemented as seen in the discrepancy of the performance of $N$-stable and $N-1$-stable capacity sets when triggering fused nodes. Also of interest in such results is the observation that during an increase in the size of the concentric attacks, the level of damage may increase, then again decrease as the number of attacks nodes is further increased. This is seen in the $N-1$-stable capacity set from an attack on approximately 100 to 110 nodes. This suggests the existence of dominating modes of cascading failures that occur for various attack configurations, yielding the same levels of damage.

2.5.6 Efficacy of Stochastically Generated Capacity Allocations

In Fig. 2.22 we study the efficacy of stochastic capacity allocations over the $N$-stable UCTE network configuration. The red data points depict the vulnerability of the $N$-stable UCTE network to attacks, and the green data points show attacks
on the same network with the best stochastically allocated capacity distribution, against nine-random-node attacks over the entire network. In Fig. 2.22(a) they are ordered by \( G \) of the stochastic capacity distribution and in (b) we show the trials ordered by \( G \) of the \( N \)-stable capacities. We stochastically search for the capacity allocation that provides the highest protection to the network in case of nine-center-node attacks starting with the \( N \)-stable capacities as the base set. Next, we use the best allocation to generate the capacity configuration of various systems, and analyze their robustness in response to nine-random-node failures in the entire network. The purpose of this procedure is to understand whether the capacity configuration that enables a highly robust network under one fixed attack will also perform well under random attacks. We find that the stochastic optimization allocation makes the network more vulnerable to random attacks/failures. This implies that by increasing the protection of the systems against a known attack strategy, we reduce the stability of the system against unforeseen attacks.

**Figure 2.22:** Stochastic capacity allocation optimization for \( N \)-stable UCTE network. The red data points depict the stability of the (a) \( N \)-stable UCTE networks against 9 random node removal from the entire network. (b) Trials ordered by \( G \). The green data points highlight the vulnerability of the network, if we add on top of the initial capacity allocation the best stochastic capacity allocation against 9 center node removals.
2.5.7 Greedy and Spatially Correlated Attack Strategies

In Fig. 2.23 we elucidate the process of finding the most damaging nodes by implementing a greedy search selection strategy. After using the greedy selection strategy to find the two most damaging nodes, in (a) we analyze the damage resulting in the failure of the 2 most damaging nodes with each remaining node in the network; (b) the damage resulting in the failure of the 3 most damaging nodes with each remaining node in the network, where the third node is that found in (a). The green lines represent the size of surviving giant component in case of the removal of (a) the 2 most damaging nodes simultaneously; (b) the 3 most damaging nodes simultaneously. These simulations were performed on the $N$-stable UCTE network with a base tolerance $\alpha=0.5927$.

![Graphs showing greedy selection of nodes](image)

**Figure 2.23:** Greedy selection of (a) 2 most damaging nodes with every other node; (b) 3 most damaging nodes with every other nodes. The green lines represent the size of surviving giant component in case of the removal of the (a) 2 most damaging nodes only; (b) the 3 most damaging nodes only. Simulations performed on $N$-stable UCTE network with $\alpha=0.5927$.

Due to the nature of the greedy selection of the most damaging nodes, the failure of an extra node is likely to have no effect, or to reduce the damage induced in the network. The particular nodes are chosen in such a manner that their effect on the load redistribution, and topology changes they induce in the network are as damaging as possible, and any perturbation in this scheme are unlikely to increase the level of damage.
Figure 2.24: Five-center-node attack. From the 9 center nodes we attack 5 different nodes for each simulation, leading to 126 possible combinations. Simulations performed on $N$-stable UCTE network (black) with $\alpha=0.5927$ and $(N-1)$-stable UCTE network (red) with $\epsilon=0.1$.

In Fig. 2.24 we attack a different set of 5 nodes selected from the nine center nodes for each simulation, leading to $\binom{9}{5} = 126$ possible combinations. Simulations performed on $N$-stable UCTE network (black) with $\alpha=0.5927$ and $(N-1)$-stable UCTE network (red) with $\epsilon=0.1$. We again observe a bimodal distribution of cascade sizes which can be attributed to cascades originating in a localized region. Such results indicate that bimodal distributions are not attributes of the properties of the failing nodes, but attributes linked to the origin of the initiation of the cascades.

2.5.8 Cascade Severity Measures ($G$ and $S$)

In Fig. 2.25 $S$ represents the number of failed nodes throughout the cascade process, whereas $G$ is the size of surviving giant component. In order to compare two forms of similar information (size of damage), we plot $1 - G$, that is the fraction of failed nodes. In Fig. 2.25(a) we observe the severity of single-node failures and in (b) the severity of four-spatially-clustered-node removals. These simulations were performed on $N$-stable UCTE network with $\alpha = 0.5927$. We show that there exists a strong linear correlation between $G$ (surviving giant component) and $S$ (number
of failed nodes), for both single and multi-node attacks, thus we can use these two measures interchangeably to quantify the severity of a cascade.

![Figure 2.25: Correlation analysis of $S$ vs. $G$. $S$ represents the number of failed nodes throughout the cascade process, whereas $G$ is the size of surviving giant component. In order to quantify the same information (size of damage), we plot the $1-G$ that is the fraction of failed nodes. (a) The severity of single node removal; (b) severity of 4 spatially clustered node removals. Simulations performed on $N$-stable UCTE network with $\alpha = 0.5927$.](image)

### 2.5.9 Analysis of First and Second Largest Giant Components

In Fig. 2.26 we observe cascades triggered by the removal of the highest load node on RGG networks of size (a) $N = 1000$, (b) $N = 2000$, (c) $N = 3000$, (d) $N = 10000$ and average degree $\langle k \rangle = 10$. $G_1$ is the size of the largest resultant giant component after the network reaches equilibrium, whereas $G_2$ is the size of the second largest giant component. We study the correlation between their sizes as a function of $\alpha$ by removing four-center-nodes from the UCTE network, similarly to the RGG networks presented in Fig. 2.18.

It is apparent that both $G_1$ and $G_2$ are immediately impacted by the phase transition, and it becomes apparent how the network is fragmented for larger cascades and lower tolerances ($\alpha$). For small tolerances, the network generally breaks into two components of similar size, indicating that segments besides the giant component don’t disintegrate, but maintain some relevant structure. Beyond the phase
transition the size of the giant component is nearly the size of the entire network. This leaves very few nodes two generate a second largest component and as expected there is an immediate drop in the size of the second largest component. Such results come as no surprise.

In Fig. 2.27 we observe (a) the surviving giant component sizes ($G_1$) in ranked order, (b) the second largest component ($G_2$) in ranked order, for all single-node failures in the UCTE network, with a capacity threshold $\alpha = 0$. Of interest is the discontinuity found in ($G_1$) for giant components with sizes approximately 800 nodes that is absent from ($G_2$). The same principles that promote a bimodal distribution in other cascade scenarios are likely responsible for this behavior in ($G_1$). The gap in ($G_1$) can not be attributed the region in which the cascade was induced, as the set of initiators spans all possible nodes. In (c) we observe the surviving giant component size ($G_1$) and the second largest component size ($G_2$) as a function of
capacity threshold $\alpha$ under a four-center-node attack on the UCTE network. A phase transition is visible for both components, similar to what was observed in Fig. 2.18.

![Figure 2.27](image)

**Figure 2.27:** Comparison of surviving giant component and second largest surviving component. (a) The surviving giant component in ranked order, (b) the second largest component in ranked order, as each single node in the UCTE network is individually attacked, with a capacity threshold $\alpha = 0$. (c) The surviving giant component size ($G_1$) and second largest component size ($G_2$) as a function of capacity threshold $\alpha$ under a 4 center node attack on the UCTE network. A phase transition is visible.

### 2.5.10 Failures Near the Phase Transition

We analyze the power-law trend of the cascade size distributions of the UCTE network in three regions: for $\alpha$ values below the phase transition, around the phase transition and above the phase transition. We find that around the phase transition region the cascade size distributions exhibit clear power-law behavior. However, as we move away from the phase transition region (both above and below), we can see the power-law trend vanish. For comparison, we have performed the same analysis
Figure 2.28: Power-law trend around the phase transition region in $N$-stable UCTE network. Comparison shown for 4 random node removal and 4 clustered node removal for various $\alpha$ values: below ($\alpha = 0.6$), around ($\alpha = 0.8$) and above ($\alpha = 1.2$) the phase transition region.)
on RGG networks, and found similar characteristics. These results are backed by theoretical findings suggesting that power-law behavior can be observed for order parameters of systems near second-order phase transitions. Critical exponents can be used to quantify the behavior of such order parameters.

Figure 2.29: Power-law trend around the phase transition region in RGG network of size $N = 1000$ and $\langle k \rangle$. Cascades triggered by the removal of single nodes for various $\alpha$ values: below ($\alpha = 0.15$), around ($\alpha = 0.45$ and $\alpha = 0.50$) and above ($\alpha = 0.65$) the phase transition region).

In Fig. 2.28 we observe cascade size distributions in the $N$-stable UCTE network. We compare distribution sizes of four-random-node failures and four-clustered-node failures for various $\alpha$ values: below ($\alpha = 0.6$), around ($\alpha = 0.8$) and above ($\alpha = 1.2$) the phase transition region. Findings are plotted on a log-log scale. The results are fairly consistent. Near the phase transition region we start to see a
linear trend on the log-log scale, suggesting the existence of a power-law distribution. Above this transition region the trend disappears, while below the transition region we observe what may likely be an exponential distribution of cascade sizes, again indicating that this is not within the phase transition.

We repeat similar simulations on a synthetic RGG network of size $N = 1000$ in Fig. 2.29. Cascades were triggered by the failure of single nodes for various $\alpha$ values above, below, and at the phase transition region. Below the phase transition ($\alpha = 0.15$), we observe a seemingly exponential distribution. Approximately at the phase transition ($\alpha = 0.45$ and $\alpha = 0.50$), we observe seemingly power-law distributions, and above ($\alpha = 0.65$) the phase transition region we observe a breakdown in the distribution where the system completely survives in under nearly all single node attack scenarios.

In Fig. 2.30 we analyze the cascade distributions for RGG networks of various system sizes and fixed average degree $\langle k \rangle = 10$. Cascades are triggered by single node failures for two $\alpha$ values near the critical region ($\alpha = 0.45$ and $\alpha = 0.50$). We find that nearly all fits near the phase transition region can be approximated by a power-law with a critical exponent of approximately 1. The size of the system has no impact on this exponent as should be expected for sufficiently large system sizes. It seems that the choice of $\alpha$ has no effect on the exponent either, but this is of course dependent on the choice for $\alpha$ being sufficiently close to the phase transition region.

### 2.5.11 Correlations in Single and Multi-Node Failures

Next, we analyze the predictability of cascading failures in the UCTE network triggered by multiple random node failures based on the knowledge of the severity of each cascading failure that each node causes individually. We show that when the number of triggering nodes ($n$) is small ($n \leq 4$) we can accurately predict the severity of induced damage. However, as the number of nodes that trigger the cascade increases, the predictability becomes ineffective.

In Fig. 2.31 we observe the correlation between surviving giant component sizes for all possible single-node attacks on the UCTE network for competing values
Figure 2.30: Power-law fits around the phase transition region in RGG networks of various system sizes and \( \langle k \rangle = 10 \). Cascades triggered by the removal of single-nodes for various \( \alpha \) values: at the critical region \( (\alpha = 0.45) \) and beyond \( (\alpha = 0.50) \).
Figure 2.31: Correlation between surviving giant component sizes for all possible single node attacks on the UCTE network with two $N$-stable capacity thresholds as represented on the axes.

of $\alpha$ under $N$-stable capacity thresholds as represented by the two axes. On the y-axis we plot the performance of the larger of the capacity thresholds, and we consistently see that the data points are more heavily concentrated on the left of the line $y = x$ indicating that the severity of induced damage is generally smaller for the higher tolerance. The results are more predictable when at least one of the tolerances in questions is near the phase transition region. We find that being at, or beyond the phase transition promotes the robustness of the system. This is expected as the emergent behavior becomes pronounced around the phase transition region. As shown in (c) the predictability decreases when the tolerances are both far from the transition point. We observe a high level of non-monotonicity in the system where higher capacity expenditure results in a decreased robustness against single-node failures. When the tolerances are well beyond the phase transition region, it is expected that the robustness of all capacity configurations will be high, and result in a clustering of the resulting data points.
Figure 2.32: Correlation analysis of multi-node attacks and the sum of individual damage each initiator node induces in $N$-stable UCTE network (small-range).

In Fig. 2.32 we perform a correlation analysis of multi-node attacks against the sum of the individual damage each initiator node induces individually in a $N$-
stable UCTE network. We use both damage metrics, $S$ and $G$, to evaluate the level of damage. For small multi-node attacks we find a strong correlation between $G$ and $\Sigma G$ as well as $S$ and $\Sigma S$. The number of outliers increases as the size of the multi-node attack is increased, indicating a decrease in the correlation. This can be attributed to a higher level of change in the topology of the network when under attack from a larger set of nodes. For multi-node attacks of size 4 or less, we see that the correlation is very strong, and that damage induced by single-node failures can be used to estimate the severity of cascades induced by multi-node attacks.

In Fig. 2.33 we look at similar results, but for larger multi-node attacks of sizes 5, 6, 7 nodes. We find that the number of outliers dramatically increases from the amount found for the smaller multi-node attacks indicating a much weaker correlation. The correlations when viewed by $S$ or $G$ show similar behaviors, as these methods have high correlation to each other as well. We see that in the range of multi-node attacks induced by $5 - 7$ nodes, using the damage from single-node failures to predict their severity is no longer reliable.

In Fig. 2.34 we analyze the correlation between multi-node attacks and the sum of individual damage each initiator node induces in $N$-stable UCTE network for multi-node attacks with the simultaneous failure of 8, 9 nodes. We see that at this point, the correlation between $G$ and $S$ is extremely weak.

In Fig. 2.35 we perform an analysis of the number of failed nodes $S$ in failures triggered by the removal of a set of 4 nodes on the UCTE network with a relative tolerance $\alpha = 0.5927$ for 300 random samplings. We perform the analysis for (a) sets of 4 clustered node failures, and (b) sets of 4 random node failures. After eliminating outliers for sets of 4 clustered nodes we find an $R^2$ value of 0.83 with no apparent bias in the data set, indicating a fair correlation between the sum of the damage dealt by the single node failures, and the multi-node failure damage. In comparison, after removing the outliers for 4 random node failures, we find an $R^2$ value of 0.94 indicating that the correlation between single and multi-node failures for randomly distributed failures is much higher than those for spatially clustered failures. Such findings come as no surprise, because a distributed attack on a network is likely to strike many inconsequential nodes, while a spatially concentrated attack will alter
Figure 2.33: Correlation analysis of multi-node attacks and the sum of individual damage each initiator node induces in $N$-stable UCTE network (mid-range).

the local topology in a manner unforeseen by individual node failures. The subplots in each figure indicate the outlier cutoff regions in blue, and the linear fits before
Figure 2.34: Correlation analysis of multi-node attacks and the sum of individual damage each initiator node induces in $N$-stable UCTE network (large-range).

and after the outlier removal in green. It can be seen that outlier removal is a necessary step in obtaining a strong fit to the subset of the data points that exhibit predictable behavior.

In Fig. 2.36 subfigures (a) and (b) present the sizes of the surviving giant component for the four-clustered-node removals as a function of the total load $\sum \ell$ of the initiator nodes, and as the total node degrees $\sum k$ of initiator nodes. (c) and (d) present similar results for the failures of 4 random nodes. All simulations are performed on the UCTE network with relative tolerance $\alpha = 0.60$. The objective of this analysis is to identify any existing correlations between the sum of the load of the initiating set of failing nodes and the size of the cascade, or the sum of the degree of the initiating set and the size of the cascade. The results are fairly inconclusive,
Figure 2.35: Correlation analysis of failures triggered by the removal of a set of 4 nodes. $\alpha = 0.5927$ (relative tolerance); 300 repetitions of four-random-node removals from the entire network.

but it can be said that attacks performed by sets of nodes with a small load sum will not cause damage to the network, while attacks induced by nodes with a high load sum will likely induce much damage in the network, as shown in (a, c). There is little to no correlations found in attacks induced by sums of load that are not in the extreme ranges.

In Fig. 2.37 we analyze the response of the network under various 4 node failures as a function of the relative tolerance $\alpha$ and we find that there is a monotonic trend in response to an increased tolerance. This may come as a surprise given that we usually see a discontinuity in the response of $G$ to changes in the tolerance near the phase transition region. The distinguishing factor is that we average over multiple randomly selected 4-node failure scenarios. This averaging eliminates any regional effects in the network. The elucidates the fact that the tolerance at which phase transitions occur is dependent upon the particular characteristics of a failure, and that the tolerance at which phase transitions occur can not be generalized.

2.6 Conclusion

We have studied how cascading failures induced by load redistribution caused by single- and multi-node failures on spatial networks carrying distributed flow prop-
Figure 2.36: Comparison of four-clustered and four-random-node removals. Subfigures (a) and (b) present the size of the surviving giant component for the four-clustered-node removals as the function of the total node degrees $\sum k$ of the initiator nodes, as well as the total load $\sum \ell$ of initiator nodes. All simulations are performed on UCTE network with $\alpha = 0.60$.

agate through the network. We conducted our research on a real-world power transmission network and in spatially-constrained synthetic network model, RGGs. We found that one cannot assess the severity of a damage induced by single- or multi-node attacks based on the degree or initial state load of the initiator nodes.

Furthermore, we have demonstrated that small ($n < 100$) spatially-localized attacks or failures cause a higher damage than spatially distributed, random failures. Our results indicate that intentional attacks on the network cause a more severe damage, however, providing protection to the system against particular at-
tack scenarios results in a more vulnerable system against other unexpected failures. On the other hand, when the system experiences a massive node failure ($n \geq 100$), the distributed attacks prove to be more damaging than the spatially-localized ones, suggesting that an extended random attack is more likely to find critical nodes that can induce severe damages.

We have proposed a fixed-cost stochastic capacity allocation strategy for mitigating single-node failures. In addition, we designed the $(N-1)$-stable UCTE network that remains stable in the event of any single-node failure. We demonstrated that while these methods can efficiently mitigate against single-node damage, they offer little protection in case of cascading failures induced by multi-node attacks. Specifically, for typical values of node-level tolerances ($\epsilon \approx 10 - 20\%$), $(N-1)$-stable networks can still develop large cascades for both spatially-concentrated and distributed multi-node attacks. In addition, we have shown that single-node characteristics (load, degree) offer little insight on the severity of induced cascades, and it is not apparent on which nodes one should increase protection to successfully mitigate cascading failures.

We have exposed the non-local nature of the spread of cascades. We have seen that triggering a failure in a localized region does not necessarily induce failures in the surrounding area. In contrast, cascading failures can propagate throughout the
entire network and cause failures in regions found at large spatial distances from
the targeted area. Moreover, we have shown that any small change in the target set
can cause a large variability in the size of induced damage.

Analyzing the survivability of the system by increasing the excess capacity,
we have revealed the non-monotonic behavior in both $N$- and $(N-1)$-stable UCTE
networks, and also in RGGs.

Additionally, we have shown that even for large system size RGG networks,
non-self averaging prevails; for large ($10^4$) network size the system still exhibits a
non-monotonic fluctuating behavior in $G$ vs $\alpha$. We have also found non-monotonic
behavior when analyzing the size of the surviving giant component by increasing
the number of targeted nodes. We have seen that cascade sizes exhibit bimodal
nature characterized by a first-order phase transition; in the critical regime, cascade-
size distributions follow power-law trends, behavior that vanishes as we move away
from the critical regions. Lastly, we have demonstrated that one can predict with
high accuracy the damage triggered by multi-node attacks, if the damage size that
each node can trigger individually is known. However, we have also shown that
as the complexity of the induced damage (number of failed nodes) increases, the
predictability becomes ineffective. We have also shown that even if we maintain
the same number of initiator nodes, by enlarging the geographic area on which the
attack is triggered, we obtain high variation in the size of induced damage. This
indicates that the size of the region in which the failure can occur also adds to the
complexity of the cascading failures, and hardens mitigation strategies in case of a
fixed number of node attacks or random failures in expanded regions.

In summary, we have found that traditional single-node measures, frequently
employed in network science (such as degree or load), are largely ineffective for
predicting sensitivity and severity of cascades or for mitigating against them. The
cascade behavior also exhibits fundamental non-monotonic features, very different
[30], [20] from cascades in epidemic spreading or social contagion: (i) a larger number
of nodes initially attacked may lead to smaller cascades; (ii) increasing the node (or
edge-level) tolerance uniformly across the network may lead to larger cascades, i.e.,
indiscriminately investing resources in the protection of nodes or links can actually
make the network more vulnerable against cascading failures (“paying more can result in less”, in terms of robustness). Both of these issues are implicitly (but inherently) related to existence of “fuse” lines and nodes in the network, whose identification is a computationally hard problem. We also observed that cascading failures are non-self-averaging in spatial graphs, hence predictability is poor and conventional mitigation strategies are ineffective. Further, in part related to the above, we have shown that cascade sizes exhibit large variability for small changes in the target set. It is also important to note that while the spatial propagation of the cascading failures resembles wave-like propagation features (overloads farther away from the original attack occur later) [20], [60], some non-local features are apparent of our cascade visualizations. The overload failure process is not a nearest-neighbor spreading process in the grid (by virtue of the current flow equations and the possible non-local redistribution of overloads); regions along the path of the cascade can be spared or "bypassed", while possibly giving rise to large-area outages far away from the location of the original attack.

In conclusion, we have used extensive real-world targeted node attack and random node failure scenarios to induce cascading failures on spatial networks, and analyzed their characteristics and propagation. We have introduced effective mitigation strategies to reduce the severity of damages, and presented the limits of predictability of assessing the severity of disruptions in the system, due to the complex nature of cascading failures occurring in spatially-embedded networks.
CHAPTER 3
ANALYSIS OF ANOMALIES IN THE DISTRIBUTION GRID

3.1 Anomaly Detection and Classification

3.1.1 Background

Failures of the distribution grid occur frequently and incur minor costs in the regions they transpire, with outages exceeding approximately 24 hours becoming particularly costly to civilian populations as unrefrigerated food spoils and daily routines are disrupted. The current use of technology in the maintenance of power distribution systems has much to improve from currents advancements in remote sensing devices. Current methods of maintenance are archaic and utilize very poor algorithms for identifying the locations of disruptions in the distribution grid, and for allocating resources responsible for well-being of the grid. Our objective is to enable smart utilization of data from sensor devices to identify problematic regions within the distribution grid in order to enable technologically informed delivery of such services, and reduce the likelihood of outages. We begin by identifying anomalous behavior as recorded by remote sensing technologies.

Unsupervised anomaly detection is fundamental to applications in various domains and has uses spanning fraud detection, medical use (i.e. cardiography), data leakage prevention and power systems [62]. Specific algorithms have been proposed for the purpose of unsupervised anomaly detection, each having biases making them more particularly suited for their domain application, but to date there is a lack of standardized algorithms known to particularly suit individual domains. We propose an anomaly detection algorithm to be applied to the distribution grid. We identify

Portions of this chapter may appear in an upcoming publication: Moussawi A., Crawford T., Lokhov A., Vuffray M., Backhaus S., "Automatic Detection and Classification of Anomalies in Distribution Power Grid" (To be submitted, 2018) [61]
two methods, one probabilistic and one heuristic, that using two distinct approaches identify the same anomalies in a particular data set. We compare the algorithms to find that the heuristic approach is more suited to real-time unsupervised anomaly detection.

Once anomalies are identified, they must be classified. We perform supervised classification, a well studied topic that is known to yield highly accurate results. To facilitate the process the identified anomalies are labeled by a human-observer, providing a ground truth off of which the learning algorithms will be trained. The anomalies contain unique characteristics that are quickly visually assessable. For this reason it is a simple task to engineer a set of features that are adept at distinguishing the various anomaly classes from one another. A 12 variable feature set is engineered to aid the learning algorithms in the classification process. Analysis shows that 5 of those features influence the majority of impact upon the training process. These 5 features are isolated for use in the learning algorithms and their performance is evaluated in the hopes of reducing overfitting, by decreasing the complexity of the feature space. The raw signal is also used as a high-dimensional input to the learning algorithms for comparative purposes, ensuring that the engineered features realize some benefit. Findings show that the decision tree outperforms all other learning algorithms on the LANL data set with the 12 variable feature space. It is also shown that over-fitting is minimized thought the use of the decision tree as opposed to a Random Forest or Neural Network algorithm.

3.1.2 Plan

We propose the analysis of PMU (Phasor Measurement Unit) data from the distribution grid to increase the efficiency of grid maintenance and operation. The process involves two fundamental steps; anomaly identification, and classification. Two methods are proposed for anomaly identification, both yielding similar results, one probabilistic and one heuristic. After the anomalies are identified, they are classified. The classification process is performed on a window ranging one second prior and post the occurrence of the anomaly, with feature selection being crucial to this process. Two methods are utilized for the purpose of anomaly classification
as well. The first is a heuristic thresholding model in which the relation between features for a given class is assessed and hard-coded. The second method utilizes the same set of features, and applies well known learning algorithms.

### 3.1.3 Data Resourcing

Recent improvements in technology have brought a reduction in the costs of remote sensing, and the ability to remotely monitor the performance of the distribution grid under constrained budget has become possible. The ability to utilize sensors over the distribution grid brings forth opportunities for improved maintenance and increased robustness. The sensors installed by the Department of Energy and other entities in distribution grids have the capability of tracking time, voltage magnitude, voltage angle, current magnitude, current angle, apparent power, real power, active power, power factor, frequency, rate of frequency change, and the status of a particular node. The data is recorded at a frequency of 30 hertz. For the focus of this study we utilize the voltage magnitude to identify and classify anomalies. A cursory glance at the voltage magnitude shows high levels of noise with an otherwise constant voltage, experiencing some drift and occasional anomalies.

### 3.1.4 Anomaly Detection

Two anomaly detection algorithms have been investigated for use on distribution grid voltage measurements. The first anomaly detection algorithm applied uses a probabilistic method in which the previous the seconds of voltage measurements are taken as a prior and the probability of real-time incoming data is assessed. When the probability of the occurrence drops below a learned threshold, the algorithm flags the measurement as an anomaly. To implement this probabilistic model, we implement a first order approximation. The data is presumed to be linear with some Gaussian noise; that is to say we assume that the voltage in the distribution grid can be modeled as a stochastic dynamical system. The following formula depicts the assumed model:
\[ X_{t+\Delta t} = AX_t + \xi_t \]  

(3.1)

where \(X_t\) is the state of the system at time \(t\), \(\xi\) is gaussian noise, and \(A\) is a matrix guiding the evolution of the state vector from time \(t\) to \(t + \Delta t\). Given a sufficient span of time series data, matrix \(A\) can be recovered by maximizing the posterior of the expression, which coincides with maximizing the prior as in Maximum Likelihood Estimation. This is mathematically achieved by maximizing the following probability:

\[ P(A|X,\xi) \propto e^{-\frac{1}{2\sigma^2} \sum_{t=1}^{T-1} ||X_{t+1} - AX_t||^2} \]  

(3.2)

yielding the result:

\[ \hat{A} = \left( \sum_{t=1}^{T-1} X_{t+1}X_t \right) \left( \sum_{t=1}^{T} X_tX_t \right)^{-1} \]  

(3.3)

More specifically, once the distribution of the gaussian noise is identified from the prior, the probability of an incoming signal is the product of the probability of noise associated with each data point:

\[ P(X_{t+1:s}|X_{0:t}) \approx P(\xi_t) \ast P(\xi_{t+1}) \ast P(\xi_{t+2}) \ast \ldots P(\xi_{t+(s-1)}) \]  

(3.4)

where \(t\) is the duration of the prior, and \(s\) is the duration of the posterior. The white noise is assumed to have a mean of zero, and the variance of the noise is obtained through maximum likelihood estimation. The accuracy of these results increase as a function of the number of data points \(T\) that they utilize. The results hinge on the assumption of normally distributed noise, which under naturally arising conditions is commonly observed. After \(A\) is trained and the standard deviation deduced from the prior measurements, the probability of incoming voltage signals can be assessed. This method can be computationally demanding depending on the size of the prior, but is quite successful when tested on human-labeled anomalies in the distribution grid.

The second method for anomaly detection is heuristically motivated, and ap-
plies basic statistical measures to generate a proxy for the probability of an incoming voltage signal. To achieve this, the difference between the voltage and its rolling mean is taken over a short duration (ten seconds) and divided by the standard deviation over that same duration. This generates a proxy for the probability of the occurrence of an anomaly. When the absolute value of this proxy exceeds a sensitivity threshold, the anomalies are flagged. In practice, this procedure flags many points during and shortly after the occurrence of the anomaly, but a window can be generated over which only the first of a set of anomalies is recorded. This method is not computationally intensive and can be run in real-time on incoming voltage measurements.

The heuristic and probabilistic methods identify the same anomalies for appropriate thresholds. The results are not remarkable once it is acknowledged that both are statistical methods. Both approaches directly measure the probability of incoming voltage signals, based on a prior. The major difference between the methods is that the first method is more scientifically rigorous, but when applied to the data, they both yield the same results, with the second method providing an advantage in computational complexity. Therefore for the purpose of real-time anomaly detection the second method is favored.

3.1.5 Anomaly Classification

To perform anomaly classification, the isolated anomalies are first hand-classified by a human with domain expertise. The classification of anomalies by eye suggests that there are features whose extraction can aid the learning algorithms in the classification process. Feature selection is critical to the learning process, and with this in mind two sets of features were engineered; one with 5 variables, and one with the original 5 and an additional 7.

The basic feature set includes:

1. $V_m$: The mean of the first third of the signal.

2. $V_p$: The mean of the final third of the signal.
### Cross-Validation/In-sample Accuracy on LANL Data

<table>
<thead>
<tr>
<th>Learning Algorithm</th>
<th>5 Features</th>
<th>12 Features</th>
<th>Raw Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decision Tree</td>
<td>78.0% / 85.0%</td>
<td>84.8% / 88.5%</td>
<td>N/A</td>
</tr>
<tr>
<td>Random Forest</td>
<td>77.2% / 100%</td>
<td>80.26% / 100%</td>
<td>N/A</td>
</tr>
<tr>
<td>Neural Net</td>
<td>78.7% / 90.3%</td>
<td>82.0% / 91.3%</td>
<td>80.7% / 90.8%</td>
</tr>
</tbody>
</table>

3. **Sum_4**: Sum of signal values exceeding the signal mean.

4. **Sum_5**: Sum of signal values not exceeding $\frac{1}{3}$ of the signal mean, summed with $\frac{2}{5}$ of the minimum signal value.

5. **Num_c**: Number of times the signal crosses a specified value.

The 12 feature vector includes all features from the 5 feature set in addition to the time at which the anomaly peaked, the minimum anomaly voltage, the width of the anomaly, the mean over the whole anomaly window, the maximum voltage reading, the mean over the first quarter of the anomaly window, and the mean over the last quarter of the anomaly window. In addition to the 5 and 12 variable feature vectors, we input the voltage signal as a feature vector when using the neural networks. This serves as a baseline that we can compare to for the purpose of ensuring that the engineered feature vectors contribute to an improvement in the accuracy of the learning algorithms.

The variation observed when applying learning algorithms with 5 and 12 features is remarkable for the decision tree. Including the 7 extra features increased the classification accuracy by nearly 20%. The decision tree utilizing all 12 features shows the strongest performance in the classification process. With the 5 variable feature set, decision trees perform quite poorly. On the other hand neural networks have similar performance when utilizing either 5 or 12 variable feature vectors, but with neither can they perform as well as the decision tree. Utilizing the random forest algorithm revealed a peculiar case; constant over-fitting as can be observed by the 100% in-sample accuracy, whether given the 5 or the 12 variable feature set. The ability of the decision tree to avoid over-fitting and its strong performance with sparse data gives it a clear edge over the other learning algorithms for the
purpose of our study. It achieves the highest accuracy and exhibits the lowest levels of over-fitting.

3.2 Recovery of Dynamical System Parameters

A quantitative analysis is performed on a daily dataset consisting of power transmission variables recorded frequency of 30 hertz, including a timestamp, VoltageMag, VoltageAng, CurrentMag, CurrentAng, MW, MVAR, MVA, PF, DFDT, Freq, Status, and Digital. Due to the redundancy of the given data, 5 of these variables are isolated (Timestamp, CurrentAng, MVAR, MVA, DFDT, PF) and used for the purpose of data analysis. First, discontinuity in VoltageAng (due to equivalence of 180 and -180 degrees is accounted for by replacing VoltageAng with sin(VoltageAng). Then, data is normalized by dividing over the mean of the full data set for each variable, and dividing by the associated standard deviation. At this point, the data is smoothened by taking a rolling mean over a window of 200 data points, and relieving the data set of any data points without sufficient information. The rolling mean is not applied to sin(VoltageAng). Fig. 3.1 shows the 5 selected variables after they have been processed.

3.2.1 Methods

As a first order approximation, the data is presumed to be linear with some Gaussian noise. We model our system using equation (2.1). Given a sufficient span of time series data, matrix A can be recovered by maximizing the posterior of the expression, which coincides with maximizing the prior as in Maximum Likelihood Estimation as in equation (2.3). The accuracy of this result increases as a function of the number of data points $T$ that it utilizes. Of prime concern is the number of data points necessary to force convergence of the results. To this end, we devise a method to compute the number of necessary data samples $T$ by calculating the $L^2$-norm of the difference between two matrices $A$ recovered using different intervals of the same data set. We define the time-step $T$ to be the interval at which data samples are utilized from the data set, in multiples of minimum intervals between two data points $\Delta t$. It is reasonable to expect that when enough data points are included in
Figure 3.1: Five principal variables of the power transmission system.

Each interval, the two recovered matrices should converge, and the difference of their $L^2$-norms will approach zero. Indeed, results in Fig. 3.2 show that the difference of the $L^2$-norms of the recovered matrices approaches 0 as the number of data points used increases. This is true for both time-steps of 1 or 2.

### 3.2.2 Optimal Recovery Interval

One drawback to measuring the accuracy of parameter recovery using such a method is that there is no accountability for a change in matrix $A$ as a function of time. To remedy this drawback it is possible to sample the same data interval at each data point, with one data set taking odd numbered data points, and the other taking even numbered data points. These two unique data sets will sample approximately the same time interval. The only hindrance is that unit time-step resolution between data points cannot be achieved. In Fig. 3.3 we recover matrix $A$
Figure 3.2: Number of data points $n$, against $L^2$-norm of difference of recovered matrices $A$, where matrices are recovered from two consecutive data samples $i_{A1} \in [0, i]$ and $i_{A2} \in [i, 2i]$ for time-steps of 1 and 2.

from two interweaved data samples, one using even numbered data points in the span $i_{even} \in [0, t]$, and one using odd numbered data points in the span $i_{odd} \in [1, t+1]$. As shown in (a, b), oddly and evenly staggered data sets recover matrix $A$ with higher accuracy over a given number of data samples. This is expected because changes in $A$ should be non-existent throughout this overlapping time interval. In Fig. 3.3(c) linear regression is used to obtain the slopes of figures (a, b) and it is shown that the recovery of $A$ quickly stabilizes as the number of data points sampled increases. The linear regression is sensitive to the window size used, and it was found that a moving window size of approximately one-sixth the data set was optimal to produce reliable
Figure 3.3: Number of data points \( n \), against \( L^2 \)-norm of difference of recovered matrices \( A \).

and relatively smooth and continuous results for the regression analysis. Regression centered at 1750 data samples with a span of \( \pm 250 \) yields a slope of \(-10^{-4}\) which suggests a reliable recovery of \( A \). In Fig. 3.3(d) the standard error of regression which quickly vanishes, is presented.

Up to this point, it has been assumed that the \( L^2 \)-norm of the difference between two matrices \( \Delta A \) is an adequate measure of their similarity. For comparative purposes, the \( L^\infty \)-norm of this quantity has also been measured in Fig. 3.4. Findings show that the two norms are nearly identical, suggesting that there is a small difference in the performance of this similarity measure when confined to any Lebesgue space.
Figure 3.4: Identical to Fig. 3 (a, b) with $L^2$-norm($\Delta A$) replaced with $L^\infty$-norm($\Delta A$). Refer to caption of figure 3.

3.2.3 Evolution of Dynamical System

With an understanding of the timescale necessary to accurately recover matrix $A$ we are ready to investigate how $A$ changes as a function of time. Recall that it was assumed that the power transmission measurements could be modeled by a linear dynamical system. This assumption may still hold for local timescales, but surely not on global time scales. The strength of such a statement can be assessed by the variance in $A$ as a function of time. In Fig. 3.5 matrix $A$ is recovered over two distinct intervals, as in Fig. 3.2, but with a separation between the intervals as denoted by the X-axis, using the full set of data points available ($time-step = 1$) over each interval. A span of 1000 data points used for each realization, with separation between origin of spans increasing on the x-axis. An average is taken over 100 consecutive intervals of constant separation for each data point computed. There exists a stochastic nature among the similarity of the recovered matrices, and one sees that this level of similarity is fairly constant as a function of increasing separation over the time scale corresponding to approximately 16 minutes. The question still remains as to whether there will be significant change in matrix $A$ over larger time periods, which is further investigated in later paragraphs.

Of prime concern is the relation between the number of data samples necessary for convergence of $A$, and the size of the time-step being used. Thus far time-steps of 1 and 2 have been investigated, but for data of resolution lower than 30 hertz this may not be possible. The motivation behind such an investigation is to reveal
Figure 3.5: Measuring the change in $A$ as a function of time.

the ideal time-step $\Delta t$, corresponding to the data frequency that most accurately yields the recovery of matrix $A$ for a fixed number of data samples, or for a fixed time span $T$. In Fig. 3.6 we plot the $L^2$-norm($\Delta A$) against the number of time-steps traversed (as in Fig. 3(a)), with the only difference being that the time-step $\Delta t$ is varied. This results in a different number of samples used over a fixed time interval for varying time-steps. The lower x-axis represents the number of data samples used to recover $A$, and the upper x-axis represents the number of data samples traversed (equivalent to time with units equal to data frequency). For smaller time-steps, the $L^2$-norm($\Delta A$) is very small, and increases as the time-step increases. Throughout the varying time-steps, it can be seen that the $L^2$-norm($\Delta A$) achieves a steady reliable value at or before $T = 1500$ for all time-steps used, suggesting a maximum time interval necessary for accurate recovery of $A$ within the given time intervals. For very large time-steps the results over shorter time spans are unreliable because a very small number of data samples are used.

In Fig. 3.7 we view the same data with magnification on the y-axis. It can be observed that there is no deduced correlation between the number of data points used, and the accuracy achieved in recovering matrix $A$. Surely there exists a linear relation between time span $T$ and the number of samples used in the recovery of $A$, but by far time span is a much stronger predictor of the accuracy of recovery, as predicted by theory [63].

While Fig. 3.6 and Fig. 3.7 were originally intended to shed light on the time span necessary for recovering matrix $A$, they do offer much more in-sight. In Fig. 3.8,
Figure 3.6: $L^2$-norm($\Delta A$) as a function of time for a fixed maximum time interval $T$, and varying time-steps $\Delta t$. Number of data points used will vary.

we once again zoom with very high magnification onto the performance of the recovery process, and ask, for which time-step does the recovery make most use of the data. To answer this question, we will focus on the slope found in Fig. 3.8. A slope of 0 indicates that the recovery process has maximized the amount of information it can extract from the data, while a negative slope indicates that the process is still refining the matrix $A$. Further work will focus on using linear regression to extract and examine the slopes of these curves.

3.2.4 Granularity Vs. Recovery Window

At this point, the next question to be asked is the nature of the relation between $\Delta t$ and the time span $T$. We define $n^*$, the minimal functioning time interval over which we can recover $A$ accurately, to be the time interval at which
Figure 3.7: $L^2$-norm($\Delta A$) as a function of time for a fixed maximum time interval $T$, and varying time-steps $\Delta t$. Magnified version of Fig. 6.

the $L^2$-norm($\Delta A$) has descended below a given threshold for a significant number of data samples. In Fig. 3.9, this threshold is 0.05 and 100 samples are considered to be a significant amount. We see that as $\Delta t$ increases, the time span required increases monotonically, but not linearly.

We now shift our attention back to the analysis of the change of matrix $A$ over large time spans (30 min, 1 hour, 10 hours etc). We sample these large time spans over 5 minutes of data each, using a span of 1500 data samples to recover matrix $A$ for each $L^2$-norm($\Delta A$) data point constructed. If the system can accurately be modeled with a linear approximation, no large changes in $A$ will occur over large time differences. Results in Fig. 3.10 show that indeed over large time differences, the correlation of matrix $A$ remains nearly constant. At a cursory glance, the fluctu-
Figure 3.8: $L^2$-norm($\Delta A$) as a function of time for a fixed maximum time interval $T$, and varying time-steps $\Delta t$. Magnified version of Fig. 6 and Fig. 7.

results do not suggest a long term change in $A$, but rather do suggest that random fluctuations are pervasive.

One way of assessing the appropriate time-step is to measure how much the reconstruction of matrix $A$ is improved over a fixed time period with varying $\Delta t$. To measure this, we take the slope graph of the $L^2$-norm($\Delta A$) vs $n$ and when this slope approaches zero, the system is no longer learning from the data. The value of $\Delta t$ for which the slope tends to 0 at the latest value $n$ is the time-step in which the system is learning most from the data. In Fig. 3.11 we have plotted this slope, and what we observe is that as $\Delta t$ increases, the convergence of the slope to 0 slows down, but the point at which this convergence occurs does not change! This again suggests that the overall time span $T$, and not the number of data points used is the variable accounting for the potency in recovering $A$, yet this again leaves us in
Figure 3.9: Time span necessary to accurately recover matrix $A$ measured in units $n^*$ (period of data sample used) against the time-step $\Delta t$ (same unit scale).

the dark when assessing which time-step is most appropriate.

At this point, we attempt to assess the most appropriate time-step by calculating $\varepsilon$, defined as the normed difference of two recovered matrices $(A_{T,\Delta t_1})^{\frac{T}{\Delta t_1}}$ and $(A_{T,\Delta t_2})^{\frac{T}{\Delta t_2}}$ using two different time-steps to recover each matrix over the same period $T$. If $\varepsilon$ remains below an appropriate threshold for two different time-steps, this indicates that the recovered matrices over the two different time-steps are in agreement. In Fig. 3.12 we plot $\varepsilon$ against $\Delta t_2$ for a fixed $\Delta t_1 = 1$. We observe relatively large values and growth in $\varepsilon$ which indicates that the recovery of matrix $A$ is not reliable. This data is preprocessed by subtracting the mean and dividing by the standard deviation over the span of data that is being used.

Another method for assessing the accuracy of the recovery of matrix $A$ is to recover this matrix over two consecutive time intervals of equal length and measure
the $L^2$-norm($\Delta A$) (Y-axis), while taking a rolling mean of varying window size over the data. First, the arithmetic mean is subtracted from the data set, and the data set is divided by its standard deviation. Next, the rolling mean is taken (not subtracted) for varying window sizes (X-axis). The $L^2$-norm($\Delta A$) may achieve a minimum which will indicate that the most appropriate time-step $\Delta t$ is being used.

In Fig. 13, we observe for time intervals of 150000 data samples, that there exists a minimum in $L^2$-norm($\Delta A$) for window size $\Delta t = 18$. It is also observed that after a rise in $L^2$-norm($\Delta A$) at $\Delta t \approx 38$ there is a drop to a region nearing the minimum achieved for $\Delta t = 18$, and this is no surprise, given time-steps greater than 1 second which are likely over-smoothening the data, resulting in matrices $A$ that are similar, yet not representative of the true dynamics of the power transmission system.
To further assess the number of data points required for the recovery of matrix $A$ to converge, we recover $A$ over a period $n$, with $\Delta t_1 = 1$ and varying $\Delta t_2$ as denoted by the legend in the subfigures. We apply the same formula used in Fig. 3.13 to obtain $\varepsilon$, and we observe that $\varepsilon$ decreases as a function of number of data samples used $n$. We calculate $\varepsilon$ in intervals of 100,000 data points.

### 3.2.5 Performance on Modeled Data

At this point, it is beneficial to shift our attention to synthetic data that is generated using the Euler-Marayuma method. This will ensure help define bounds on the expectations of the accuracy of parameter recovery under the assumption that the power grid truly is a linear dynamical system. We begin by generating a stable matrix $A$ by ensuring that $Tr(A) < 0$ and $det(A) > 0$ in two dimensions. Under this scheme, we find that we can accurately recover matrix $A$, and that for
a fixed number of time steps, as the time-step is decreased, the accuracy of matrix recovery decreases. This is likely due to numerical inaccuracies. We apply a modified formula for the recovery of matrix $A$ that accounts for varying time-step $\Delta t$:

$$\hat{A} = \frac{1}{\Delta t} \sum_{t=1}^{T-1} X_{t+1}X_t \left( \sum_{t=1}^{T} X_tX_t \right)^{-1}$$

(3.5)

At this point, we use the same formula, for a 5-dimensional attribute vector. The stability requirements for higher dimension dynamical systems require more stringent conditions than those for the 2-dimensional case. For this reason we opt to not generate matrix $A$ synthetically, but to use the given data to reproduce the matrix through the use of 30,000 data points, which have $\Delta t = 30$, equaling a time length of 1000 seconds. Next we generate synthetic data. This is done by utilizing the Euler-Marayuma method in conjunction with the matrix $A_1$ recovered from the real data. We plot the $L^2$-norm($\Delta A$) vs. time. Here our $\Delta A$ is the difference be-
Figure 3.13: $L^2$-norm($\Delta A$) vs. $\Delta t$, showing a minimum for $\Delta t = 18$.

Figure 3.13: $L^2$-norm($\Delta A$) vs. $\Delta t$, showing a minimum for $\Delta t = 18$.

Figure 3.13: $L^2$-norm($\Delta A$) vs. $\Delta t$, showing a minimum for $\Delta t = 18$.

Figure 3.13: $L^2$-norm($\Delta A$) vs. $\Delta t$, showing a minimum for $\Delta t = 18$.

between the matrix $A_1$, and $A_2$ recovered from the synthetic data generated by the Euler-Marayuma method and $A_1$. In Fig. 3.15(a) we see the results when the noise in the model is set to zero, and in (b) we see the results average over 100 random samples for each data point, for noise sampled from a Weiner process with mean 0 and standard deviation $= \sqrt{t}$, as prescribed by the model.

The results from Fig. 3.15(a) show that approximately $30 \times 100 = 3000$ data samples are required to obtain an $L_2$-norm below 0.1, when the model is generated without noise. Computing $A$ directly from the data as in Fig. 3.2(b) suggests a similar number of data samples. When noise is added to the model we find that the number of data samples increases drastically as the learned parameters are obfuscated by this noise. The real data is inundated with noise. The next step is to create an Euler-Marayuma model with an amount of noise that accurately mimics the real world PMU sensor data.
Figure 3.14: $\varepsilon$ vs. $n$, for different values of $\Delta t_2$ in each subfigure.

(a) Without noise (noise = 0).  (b) With noise (noise = 1).

Figure 3.15: Measuring $L^2$-norm($\Delta A$).
4.1 Introduction

Over the past few decades, there has been interest in understanding the dynamics of first-passage occurrences in statistically dominated processes. The definition of first-passage has developed to encompass multiple mechanisms over time, but in simplest terms, it is the first occurrence of a binary change at an individual site within a system. This definition can and will be extended to non-binary systems of various types, with and without symmetrical "states". Efforts have been vested in understanding the nature of persistence in directed percolation, as evidence of a directed percolation universality class of continuous phase transitions has been established. The mechanisms driving the characteristics observed in this universality class are still under investigation. Analytical approaches seldom yield results except in constrained cases where rigid requirements are met. There is interest in identifying whether persistence in various models may be associated with a universality class.

Diffusion [64], [65], [66], and contact processes [67], [68] have been studied extensively, and critical exponents associated with persistence in these systems have been identified both theoretically and numerically.

We discuss diffusion in the simplest sense as prescribed for networks by:

\[
\frac{\partial \phi_i(t)}{\partial t} = \sum_j A_{ij}(\phi_j(t) - \phi_i(t)) \quad (4.1)
\]

and in the discretized form:

\[
\phi_i(t + \Delta t) = \phi_i(t) + \Delta t \sum_j A_{ij}(\phi_j(t) - \phi_i(t)) \quad (4.2)
\]

where \(\phi_i(t)\) reflects that value of the particle density at location \(i\) at time \(t\), and \(A_{ij}\) is the standard adjacency matrix.
We also discuss contact processes as prescribed for networks by:

\[ \partial_t \rho_i(t) = \beta(1 - \rho_i(t)) \sum_j A_{ij} \rho_j(t)(\sum_j A_{ij})^{-1} - \gamma \rho_i(t) \]  

(4.3)

and in the discretized form:

\[ \rho_i(t + \Delta t) = (1 - \gamma \Delta t) \rho_i(t) + \beta \Delta t(1 - \rho_i(t)) \sum_j A_{ij} \rho_j(t)(\sum_j A_{ij})^{-1} \]  

(4.4)

where \( \beta \) is a parameter indicating the infection rate.

Studies have investigated both global and local persistence, defined as the persistence associated with a block containing an infinite number of sites, or an individual site respectively. In dealing with global persistence, Hincrichsen [68] suggests defining this property of a system as the probability that the global order parameter does not cross its mean value, which for asymptotically trending systems will be equivalent to the steady-state value. In dealing with the local persistence we simply look at the probability associated with an individual lattice site, and we limit our study to this.

\[ P_i(t) = P(\Delta \rho_i(t') < 0 : \forall t' < t) \]  

(4.5)

The standard definition of \( \Delta \rho_i(t) = \rho_i(t) - \langle \rho_i(t) \rangle \) applies. In homogenous systems, the persistence is independent of spatial variance, and hence \( P(t) = P_i(t) \), and we can evaluate the persistence as the fraction of nodes that have not changed sign by time \( t \). For certain processes such values can be yielded analytically. We have now defined the persistence probability for a non-binary system. Secondly, we have defined the persistence for a non-symmetric system in which we consider a change to occur only when the system crosses from below to above the mean value of the order parameter. We extend this and consider crossings in both directions, such that we define two persistence probabilities, one for up-crossings, and one for down-crossings.

\[ P_i^+(t) = P(\Delta \rho_i(t') < 0 : \forall t' < t) \]  

(4.6)
We define $P_i^+(t)$ as the probability of crossing from under the mean to above the mean (up-crossing), and vice-versa for $P_i^-(t)$. For systems with field symmetry, these values are both equivalent to the total persistence.

\[ P_i^+(t) = P_i^-(t) = P_i(t) \]  

### 4.2 Persistence in Diffusive Models

Equipped with an understanding of persistence and how it is measured, we now investigate persistence in diffusive models with varying topologies. We turn our attention to Fig. 4.1 where we observe the effects of different initial conditions on persistence in a diffusive model applied to a 1-D chain with periodic boundary conditions. The initial state of the field values in the diffusive system are selected from a uniform distribution centered at zero, with a varying spread as indicated by the legend. It is observed that the spread of the uniform initial distribution has no effect on the persistence.

In Fig. 4.2 we recreate the same simulations, with the only difference being that the initial state of the system is sampled from a gaussian distribution. We arrive at nearly identical results to those obtained from an initial state sampled from a uniform distribution, suggesting that the persistence is dependent on the model dynamics and topology, not the initial state of the system. In both scenarios, we observe a linear trend on a log-log plot suggesting that the persistence exhibits a power-law decay of the form

\[ P_i(t) \propto t^{-\theta} \]  

where the observed critical exponent $\theta$ is approximately 0.12 as has been accepted in published literature.

We investigate persistence in 2-dimensional models as well, with our findings again agreeing with published literature. In Fig. 4.3 we observe results very qualitatively similar to those found in the 1-dimensional case, with a critical exponent
Figure 4.1: Total persistence, $P_i(t)$ for diffusion on a 1-D chain as a function of time (log-log scale). System initialized by uniform distribution with varying spreads as indicated by the legend.

of nearly 0.19 found for all cases.

4.2.1 Diffusion on Erdős-Rényi Graphs

At this point, we have demonstrated that the persistence exhibits invariance under varying initial conditions. Now the investigation addresses how differing topologies affect the persistence. We start by studying how the persistence evolves on an Erdős-Rényi graph of average degree $\langle k \rangle = 6$ as shown for different degree classes in Fig. 4.4, for different system sizes [69]. While for homogenous systems $P_i(t)$ is node invariant, for E-R graphs $P_i(t)$ is not node invariant and can be calculated for nodes of particular degrees. The first visible difference is that the persistence drops faster for larger system sizes. The next observable effect is that nodes with large degrees exhibit lower persistence values. This is not remarkable, as low degree nodes have very few neighbors which have the possibility of influencing them to change state.
4.3 Persistence in Contact Processes

In Fig. 4.5 we observe a log-log plot of the total persistence of a contact process. This contact process is implemented on a one-dimensional lattice with 10,000 sites, run for a total of 10,000 iterations, with a time scale $dt = 0.01$ over each iteration [69]. The lattice sites are initialized to a uniform distribution of values centered around $\phi(0) = \phi_{eq} = 1 - \frac{\gamma}{\beta}$ with a range of $\pm 0.0005$. We treat each lattice site as a densely populated region with a field value representing the particle density in the region. As seen in the figure, the linear trend over the log-log scale indicates that the persistence indeed follows a power-law distribution as has been shown theoretically and numerically [67]. The value of $\gamma$ is varied, and the persistence is measured in both the up and down directions. It is apparent that the slope is a function of $\gamma$. In Fig. 4.6 we see the persistence occurring from a cross in the upwards direction, and observe that as $\gamma$ approaches 1, the slope $\theta$ approaches a value of approximately 0.126, while in Fig. 4.7 we find that the downwards crossing persistence approaches approximately the same value as show in tables 31. - 3.3.
This indicates a point of symmetry at $\gamma = 1$ which is quite surprising given that $\phi_{eq} = 1 - \frac{\gamma}{\beta} = 0$, indicating that at the limit, it would be impossible for an upwards crossing to occur as the system approaches its steady-state. For smaller values of $\gamma$ the power-law exponent associated with upwards crossings remains nearly equivalent to that associated with downward crossings $\theta^+ \simeq \theta^-$. Interestingly, the critical exponent for total crossings seems to be approaching that found in diffusive models, as the parameter $\gamma \rightarrow 1$. This will be an area of focused investigation, as this may be an indication of a universality class for such systems. For mathematical justification of why the critical point $\gamma = 1$ observes such behavior see Appendix B.

Our investigation of diffusion in contact processes has established an agreement with the existing findings in the literature, suggesting that there indeed exists a power-law decay to persistence probabilities in such systems, and the values we have obtained in 1 and 2 dimensions are in agreement as well [64], [65]. We now extend our study of contact processes to networks, and investigate any emergent properties from such systems and how the properties may respond to various network
Table 4.1: Critical Exponent (total crossings) as a Function of $\gamma$ for a contact process on a one-dimensional lattice with 10,000 sites, run for a total of 10,000 iterations.

<table>
<thead>
<tr>
<th>$\theta$</th>
<th>$\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.12658857258610473</td>
<td>.999</td>
</tr>
<tr>
<td>0.12600701389046054</td>
<td>.99</td>
</tr>
<tr>
<td>0.12681793866999397</td>
<td>.95</td>
</tr>
<tr>
<td>0.12698172154658807</td>
<td>.9</td>
</tr>
<tr>
<td>0.12822038014176812</td>
<td>.8</td>
</tr>
<tr>
<td>0.12992666764647007</td>
<td>.7</td>
</tr>
<tr>
<td>0.1320378109471722</td>
<td>.6</td>
</tr>
<tr>
<td>0.13560889930720804</td>
<td>.5</td>
</tr>
</tbody>
</table>

Table 4.2: Critical Exponent (upwards crossings) as a Function of $\gamma$ for a contact process on a one-dimensional lattice with 10,000 sites, run for a total of 10,000 iterations.

<table>
<thead>
<tr>
<th>$\theta^+$</th>
<th>$\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.12647315059889747</td>
<td>.999</td>
</tr>
<tr>
<td>0.1256676281522528</td>
<td>.99</td>
</tr>
<tr>
<td>0.12650416513871876</td>
<td>.95</td>
</tr>
<tr>
<td>0.12721017813312202</td>
<td>.9</td>
</tr>
<tr>
<td>0.12842808046679502</td>
<td>.8</td>
</tr>
<tr>
<td>0.13010956752952302</td>
<td>.7</td>
</tr>
<tr>
<td>0.1319627524097634</td>
<td>.6</td>
</tr>
<tr>
<td>0.1352503248795213</td>
<td>.5</td>
</tr>
</tbody>
</table>

Table 4.3: Critical Exponent (downwards crossings) as a Function of $\gamma$ for a contact process on a one-dimensional lattice with 10,000 sites, run for a total of 10,000 iterations.

<table>
<thead>
<tr>
<th>$\theta^-$</th>
<th>$\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>-0.1267039296113703</td>
<td>.999</td>
</tr>
<tr>
<td>-0.12634709342126932</td>
<td>.99</td>
</tr>
<tr>
<td>-0.12713207936510396</td>
<td>.95</td>
</tr>
<tr>
<td>-0.126753383571387376</td>
<td>.9</td>
</tr>
<tr>
<td>-0.12801264812136443</td>
<td>.8</td>
</tr>
<tr>
<td>-0.12974394597894792</td>
<td>.7</td>
</tr>
<tr>
<td>-0.1321128460627289</td>
<td>.6</td>
</tr>
<tr>
<td>-0.1359674396191164</td>
<td>.5</td>
</tr>
</tbody>
</table>
Figure 4.4: Total persistence for diffusion on an Erdős-Rényi Graph as a function of time (log-log scale). System initialized by *uniform distribution*. Persistence is evaluated for nodes of a particular degree. Run for 2 system sizes, $N = 1000$ and $N = 10,000$ characteristics. Any emergent properties successfully found, may later be applied to real world data, primarily social networks.

4.3.1 Contact Processes on Erdős-Rényi Graphs

We measure the persistence of contact processes on an ensemble of 10,000 Erdős-Rényi graphs of average degree $\langle k \rangle = 6$ over 40 time units with a time-step $dt = 0.01$ in Fig. 4.8. We observe non-trivial persistence decay in this system [69]. The poorly behaved form of this function suggests that there exists a very low possibility of analytically computing the persistence in contact processes on Erdős-Rényi graphs. These findings are similar to those found for diffusion on Erdős-Rényi graphs and suggest that it is the network structure as opposed to the dynamics of the spreading process which are responsible for the non-trivial decay of the persistence.
Figure 4.5: Total persistence of a contact process on a 1-D lattice $P_i(t)$ as a function of time (log-log scale). 10,000 lattice sites, 10,000 iterations, and time scale $dt = 0.01$.

Figure 4.6: Up-crossing persistence of a contact process on a 1-D lattice $P_i^+(t)$ as a function of time (log-log scale). 10,000 lattice sites, 10,000 iterations, and time scale $dt = 0.01$. 
Figure 4.7: Down-crossing persistence of a contact process on a 1-D lattice $P_i^-(t)$ as a function of time (log-log scale). 10,000 lattice sites, 10,000 iterations, and time scale $dt = 0.01$.

Figure 4.8: Up-crossing, down-crossing, and total persistence for a contact process on an Erdős-Rényi graph as a function of time (Semi-Log scale). System initialized with uniform distribution.
4.4 Complete Graphs

Complete graphs offer analytically tractable solutions due to their topological simplicity and high-degree of symmetry. Toroczkai was successful in finding iterative solutions to the dynamics of diffusion on complete graphs, and in identifying their asymptotic behavior. It was found that for finite systems, the fields at the lattice sites reach some equilibrium value that is not necessarily zero. As system size approaches infinity the equilibrium value approaches zero [69]. As for persistence, it was found that due to the extreme connectivity of complete graphs, the value either crosses the zero point during the first time step, or else it never will. Thus, persistence on complete graphs is virtually independent of time, and it was further shown that the persistence probability is equal to $\frac{1}{2}$. Computational results performed through Monte Carlo simulation are in agreement with the findings of Toroczkai [69]. In Fig. 4.9 we see exactly what was prescribed. The dynamics all occur within the first time step, and the persistence approaches $\frac{1}{2}$. We also observe the persistence for sites with initially negative, and positive values separately. We find that they vary round the $\frac{1}{2}$ mark but follow the predicted dynamics. In Fig. 4.10 we see that for a different set of simulations, the up and down crossing persistence change orientation relative to the total persistence, indicating that this is merely a statistical effect and that as the number of simulations approach infinity the values of all forms of persistence should approach $\frac{1}{2}$.

4.5 Conclusions

We find that persistence in diffusive systems and in contact processes on networks and lattices behave predictably and in agreement with what has been published in the literature. Although most work in the literature has thus far focused on diffusive processes, the agreement found with contact processes is likely due to the topology of networks being the determining factor of a systems persistence, more so than the dynamics of the underlying process driving the persistence of nodes. This is surprising given that the persistence is directly linked to and arguably governed by the dynamics of the system. At the same time this is also very exciting because it hints at deeper level concepts at play, likely the same concepts that are responsible
Figure 4.9: Up-crossing, down-crossing, and total persistence on Complete graphs (semi-log scale).

Figure 4.10: Up-crossing, down-crossing, and total persistence on Complete graphs (semi-log scale).

for the similarity in responses of systems within the same universality classes.
CHAPTER 5
CONTRIBUTIONS AND FURTHER RESEARCH

The research conducted in this dissertation has spanned from the study of cascading failures in power transmission grids, to the study of anomaly detection in distribution grids, and the study of persistence in networks. The study of cascading failures in power transmission grids has shed light on the relation between single-node and multi-node induced cascading failures, and has shown how the propagation of cascading failures is affected by different initial failures schemes. Mitigation strategies for such failures were also investigated, and it was shown how under constrained costs, improved capacity allocations can be achieved under the $N$-stable and $(N-1)$-stable capacity schema. Finally, a study of the current total capacity allocation in real world power grids has shown that these systems are allocated an amount of capacity leaving them in a critical regime in which cascade sizes follow a power law distribution. These findings were verified through Monte-Carlo simulation on the UCTE (European) power transmission grid.

The study of anomaly detection and classification is still in its infancy. Thus far, we have proven successful in identifying anomalies, and our ability to classify them with given precision, recall, and accuracy. The next step is to look at outages in the distribution grid and correlate them with the occurrence of anomalies, and to study the coefficient matrix $A$ and to analyze its behavior during incipient anomaly occurrences. This work is being followed up on by two researchers at Los Alamos National Labs.

Finally, the study of persistence in networks is also in its infancy, but the results are promising. It has been found that different dynamics models applied to a single graph topology reproduce the same critical persistence exponents suggesting a deeper meaning to the universality classes with which they are associated, and a strong link to network topology. None of the aforementioned research could have been performed without the mentorship and assistance of many individuals, and the research has resulted in many open questions. This chapter will help inform
the reader where current efforts in the research are headed, and what contributions were made by the various contributors.

5.1 Future Research

The study of cascading failures in power grids presented in the first chapter showed the limits of predictability in the outcomes of these failures. Most of the research focused on analyzing the initial conditions of the system, and trying to draw relations between the final outcome of the cascading failure. The main drawback of such approaches is that the correlations found for cascading failures in spatially embedded networks are extremely weak. This occurs in spatially embedded networks due to fractures in the topology of the network incrementally changing the network topology. This adversely affects the load distribution in the network in such a way that it greatly deviates from the load distribution of the intact network. To address this issue and to understand how topological changes affect the redistribution of load and the propagation of the cascades, we have to consider the state of the network at each step. In other words we need to track the progression of a cascade after each individual overload occurs. There is likely to be stronger correlations between two consecutive states in the cascade, than between the initial and final state. In addition we neglect to account for AC power dynamics, and transient states that exist during the change of network topology as failures occur in the power grid [28], [29].

The work performed at the Center for Non-Linear Studies in Los Alamos National Laboratory on anomaly detection and classification in the distribution grid is still an effort in progress. At this point, successes have been found in anomaly detection and in the classification of anomalies based on classes diagnosed by a domain expert. The link between the occurrence of anomalies, and outages in the distribution grid has yet to be investigated. It is expected that sets of anomalies can be indicative of particular outages. Sufficient amounts of data on the occurrence of outages in addition to classified anomalies need to be studied in order to make progress in this direction. The anomaly detection and classification algorithms are currently being updated by a researcher at the Center for Non-Linear Studies, and another researcher is investigating the changes of matrix elements of the dynamic
coefficient over time, to try to understand how the elements of this matrix behave when an anomaly is incipiently occurring.

Finally, the third chapter discussing persistence in networks has been an endeavor based on the initial work of previous graduate students, as well current work by Melinda Varga. The research thus far is still in its infancy, but the results are quite promising. It has been found that both diffusion and contact processes in a given regime on a given network result in the same critical exponents for persistence. This research has been extended to networks with different topologies as well, showing that the topology has a strong effect on persistence. The next step in this research is to identify what factors affect the decay of the persistence probability, and why many different models seem to fall in the same universality class. A strong understanding of what mechanisms are at play could validate the use of persistence models for the study of opinion change in social systems. Given the complexity of persistence in networks, most solutions are unlikely to be analytically tractable, and with the abound amounts of computing power available today we hope to continue and expand on much of the work that was published in the late 20th century.

5.2 Contributions

The work presented in this thesis was a collaborative effort. It was pursued and completed under the assistance and guidance of mainly György Korniss, Boleslaw Szymanski, Noemi Derzsy, and Xin Lin. Other contributors assisted in smaller degrees than these individuals. György Korniss and to an extent Boleslaw Szymanski gave high-level insight on how to approach the research, how to validate findings, and assisted in developing new methodologies for addressing research objectives. These contributions are found in the first and third chapters. Noemi Derzsy was a major contributor to the first chapter, and assisted in many of the theoretical results obtained through Monte Carlo simulation on synthetic networks. These findings were instrumental for understanding how change in topology affected our research findings, and served as great comparative results. Xin Lin was also a significant contributor to the first chapter and performed simulations on the UCTE network. The research performed in the second chapter was performed under the guidance of
Marc Vuffray, Andrey Lokhorv, and Scott Backhaus at the Center for Non-Linear Studies of the Los Alamos National Laboratory. The research performed in the third chapter has been aided by the help of research performed by David Hunt, and Melinda Varga while the research has been guided by György Korniss, Boleslaw Szymanski, and Zoltan Toroczkai.
APPENDIX A
Probability Estimation and Parameter Recovery in
Stochastic Dynamical Systems

A.1 Parameter Recovery

We define a linear stochastic model of the form

\[ X_{t+1} = AX_t + \xi_t \] (A.1)

where \( X_t \) is the state of the system at time \( t \), \( A \) is the coefficient controlling the evolution of the state of the system, and \( \xi_t \) is gaussian distributed noise exhibited in the system at time \( t \).

We assume a uniform prior on \( A \), such that

\[ P(A|X,\xi_t) \propto e^{\left(-T^{-1}\sum_{t=1}^{T}||X_{t+1} - AX_t||^2\right)/2\sigma^2} \] (A.2)

and for unregularized regression, we minimize the loss function over our coefficient \( A \) where the assumption of white noise becomes crucial. This can be achieved through minimizing mean squared error as in maximum likelihood estimation, which happens to be equivalent to maximum a posteriori estimation for this case.

\[ \hat{A}_{MME} = \hat{A}_{MAP} = \arg\min_A \sum_{t=1}^{T-1} ||X_{t+1} - AX_t||^2 \] (A.3)

yielding the result:

\[ \hat{A} = \left( \sum_{t=1}^{T-1} X_{t+1}X_t \right)\left( \sum_{t=1}^{T} X_tX_t \right)^{-1} \] (A.4)

The accuracy of the recovery of the parameter \( A \) is crucially dependent upon the time interval between consecutive samples, and the duration over which the parameter is recovered.
A.2 Probability Estimation

We assume Markovian dynamics for the progression of the state of our system, enabling assumptions that simplify probability calculations.

\[ P(X_{[1:t]}) = \prod_{i=0}^{T-1} P(X_{i+1}|A, X_i) \]  

(A.5)

The key here is that the system learns the parameters \( A \) and \( X_i \) over previous time steps \( i \), and assuming white noise of a given mean and standard deviation, is able to calculate the probability of the next data sample \( X_{i+1} \).

Again we rely on the Gaussian form of the white noise to realize

\[ P(X_{i+1}|X_i, A) = P(\xi_{i+1}) \]  

(A.6)

and thus we can conclude that

\[ P(X_{[t+1:s]}|X_{[0:t]}) \simeq \prod_{i=t}^{i=t+s-1} P(\xi_i) = P(\xi_t) * P(\xi_{t+1}) * P(\xi_{t+2}) * ... P(\xi_{t+(s-1)}) \]  

(A.7)

showing that the probability over a set of incoming data samples can be estimated by the noise distributions of those samples, under the assumption that the parameter \( A \) recovered over the prior accurately described the evolution of the system, and had minimal change over the interval \([0 : s]\).
APPENDIX B
Steady-State Behavior of the SIS Model Through Mean Field Approximation

B.1 Loss of Persistent Sites in SIS model

We begin with the generalized mean field approximation for the SIS model

$$\partial_t \phi(t) = \beta \phi(t)(1 - \phi(t)) - \gamma \phi(t) \quad (B.1)$$

where we define $\phi$ to be the infection density. This equation can be solved analytically, yielding equilibrium values for infection density. We denote the initial infection density $\phi(0) = \phi_0$ and find

$$\phi(t) = \frac{1 - \gamma/\beta}{1 + (1 - \gamma/\beta) e^{-(\beta - \gamma)t}} \quad (B.2)$$

The equilibrium value for the steady state in the regime where $\beta < \gamma$ can be found to be $\phi_{eq} = 0$ by taking the limit $t \to \infty$ in which case the exponential in the denominator diverges. This result is expected given that the system relies on infected sites to spread infection, and therefore a recovery rate greater than the infection rate sends the system into a fully recovered state in which no more infections can occur. The more interesting behavior is observed for the steady-state in which the infection rate is greater than the recover rate ($\beta > \gamma$). In this regime the equilibrium value is non-trivial. Again taking the limit as $t \to \infty$, we find that the exponential in the denominator approaches zero, leaving the system in an equilibrium state $\phi_{eq} = 1 - \gamma/\beta$. In this regime, the infection rate is strong enough to sustain itself indefinitely, while the recovery rate keeps the system from approaching a fully infected state.

Of greatest interest is the behavior of the system as the infection and recovery rates are close to convergence $\beta \to \gamma$. Through careful analysis we find that in this regime the decay of the infection density is much slower than observed for the $\beta < \gamma$
steady-state

\[ \phi(t) = \frac{1}{1/\phi_0 + \beta t} \tag{B.3} \]

or in the steady-state

\[ \phi(t) \approx \frac{1}{\beta t} \tag{B.4} \]

following a power-law decay in the large \( t \) limit where \( t \gg \frac{1}{\beta \phi_0} \).

We now turn our attention to persistent sites (defined as sites that have not yet become infected). We note that the dynamics of the SIS model dictate that susceptible sites become infected at a rate proportional to \( \beta \) and the infection rate \( \phi \). Thus, given a density \( \psi \) of persistent sites, the evolution of this density follows

\[ \partial_t \psi(t) = -\beta \phi(t) \psi(t) \tag{B.5} \]

where we impose boundary conditions \( \psi(0) = 1 \) and \( \psi(1) = 0 \).

Now we specifically address the behavior of persistent sites in the steady-state, and the regime where \( \beta \to \gamma \). Using the results found in eq. B.3 in conjunction with eq. B.5 we find the decay in the number of persistent sites to be

\[ \psi(t) = \frac{\psi_0}{1 + \beta \phi_0 t} \tag{B.6} \]

where \( \psi(0) = \psi_0 \).

### B.2 Fluctuations about the Endemic State

We now study fluctuations about the endemic state, by considering interactions between neighboring sites in our network. For illustration, we focus our attention on 1-dimensional lattices, and use the discrete formulation of the SIS model.

\[ \partial_t \phi_i(t) = \beta (1 - \phi_i(t)) \frac{\phi_{i+1}(t) + \phi_{i-1}(t)}{2} - \gamma \phi_i(t) \tag{B.7} \]

At equilibrium, \( \phi \) is constant and independent of location. Applying this to the discrete formulation we find that two equilibrium states exist. One trivial,
\[ \phi_{eq} = 0 \quad \text{for} \quad \beta < \gamma \quad \text{(B.8)} \]

and the endemic state,

\[ \phi_{eq} = 1 - \frac{\gamma}{\beta} \quad \text{for} \quad \beta > \gamma \quad \text{(B.9)} \]

We now investigate small fluctuations about the endemic state by explicitly identifying fluctuations about the equilibrium state by decomposing \( \phi \),

\[ \phi_i(t) = \phi_{eq} + \rho_i(t) \quad \text{(B.10)} \]

we assume that \( \rho \) is small, allowing us to ignore terms that are of second order, and after some simplification we find that

\[ \partial_t \rho_i(t) = \frac{\gamma}{2} (\rho_{i+1}(t) + \rho_{i-1}(t)) - \beta \rho_i(t) \quad \text{(B.11)} \]

explicitly showing the dynamics of the fluctuations about the endemic state.
REFERENCES


[54] Q. Zhou and J. W. Bialek, “Approximate model of european interconnected system as a benchmark system to study effects of


