Spatiotemporal network resilience engineering

Fernando Kuipers
Delft University of Technology
https://fernandokuipers.nl/

Joint work with (former) PhD students:
- Jorik Oostenbrink
- Farabi Iqbal
- Stojan Trajanovski
Amazon’s cloud services

Amazon Cloud Failure Takes Down Web Sites

By CLAIRE CAIN MILLER  APRIL 21, 2011 4:40 PM  ▪  19 Comments

10:28 a.m. | Updated to reflect status of the problem on Friday.

A widespread failure in Amazon.com’s Web services business was still affecting many Internet sites on Friday morning, highlighting the risks involved when companies rely on so-called cloud computing.

The problems, which began early Thursday morning, affected sites including Quora.com, Reddit.com, GroupMe.com and Scvngr.com, which all posted messages to their visitors about the issue. Most of the sites have been inaccessible for hours, and others were only partly operational.
Blackberry’s switch failure
RIM global outage caused by core switch failure; fix under way

Backup system also didn’t work, RIM explains

BlackBerry service delays experienced by users around the world on Tuesday were caused by a core switch failure within the infrastructure of Research In Motion (RIM), the company said late Tuesday.

A RIM spokesman said service was beginning to be restored to normal around 2 p.m. Eastern time, although there would be further delays as backlogs in data are cleared. It was the second outage -- or "delay," as RIM put it -- in two days affecting users in numerous countries.

RIM’s system is designed to failover to a backup switch, but the failover system "did not function as previously tested," according to a statement issued by RIM at 5 p.m. Eastern time.
Hurricane Sandy (Oct. 2012)

Hurricane Sandy doubled failures in US internet infrastructure

US internet infrastructure was severely affected by Hurricane Sandy, researchers have found, and providers took days to recover from the damage caused by the extreme weather.

Internet failure taxonomy

- Large-scale Internet (service) failures occur regularly [1]:
  - Co-dependency on multiple systems (e.g., clouds)
  - Deployed protection schemes can’t cope with disasters, such as hurricanes and earthquakes
  - Higher network utilization (e.g., via SDN), means less backup resources (and new vulnerabilities)

Global risks

- World Economic Forum [1]:
  - Cyberattacks and Critical information infrastructure breakdown are the most impactful technological risks
  - The two most likely risks to occur are that of (1) extreme weather events and (2) natural disasters
- Disasters should be given highest priority

Where disasters strike…
The critical regions problem

• How to determine the vulnerability of a network to the failure of a certain region in which it is partly embedded?

• Given a region of certain shape, where would it have to fail to inflict the gravest damage to the network?

Source: National Hurricane Center

Finding critical regions

Which region is most critical?
Finding critical regions

This one?

Which region is most critical?
Finding critical regions

Or maybe this one?

Which region is most critical?
Finding critical regions

Or one of these two?

Which region is most critical?
Algorithm: Covering a set of nodes

- If there exists a circle that covers a set of nodes $S$, then that same set $S$ can also be covered by a circle of the same size that passes through 2 nodes in $S$

- Hence we only need to consider $O(N^2)$ pairs of nodes each representing two possible circles ($N$: # nodes)
Method applicable to other shapes

But now we need to consider combinations of 3 nodes!
Critical regions European backbone

London area is most “critical”
Fortifying networks
Augmentation by $k$ links is NP-complete
- Heuristic: Add 1 link that realizes the greatest reduction in network degradation after failure of the critical region
  - Repeat $k$ times
Region-disjoint paths problem

- Find two paths between a source-destination pair, such that the failure of any region (excl. source & destination) cannot cut both paths simultaneously
- Only the diameter of a figure counts, so we can use a circle
- NP-hard problem
Region-disjoint paths heuristic

- Run node-disjoint paths algorithm to find $P_1$ and $P_2$
- Find critical pairs $K$ (a pair of nodes too close to each other)
- Divide all nodes in two sets based on proximity to $P_i$, $i = 1, 2$
- Find node $k$ in $K$ that appears in most of the pairs
- “Fix” this part of $P_i$ by finding a detour
- Repeat until there are no nodes in $K$
Region-disjoint paths results

(a) ARPANET

(b) Italy

(c) Europe
Not only nodes have geo-information, so do links…
The geography of links [1]

- Spatially-close links (e.g., along a bridge) have a high chance of failing simultaneously.
- Previous network resilience research considered all links to be straight lines between two nodes.

Link representation

- Concatenation of multiple link segments of varying length
- Each link segment is a straight line connecting two points of known geodetic location
Spatially-close intervals

- The longer the interval over which links are spatially close, the higher the risk of failing simultaneously
Risk groups

A risk group is a set of links that are spatially close to every other link in the same set.
Algorithmic problems

• Detection of spatially-close link segments: Given a network, find all pairs of link segments that are less than $\Delta$ apart

• Spatially-close intervals: Given a link $x$ and a set of other links, find the intervals of link $x$ that are spatially close to any link in the set of links

• Risk group assignment: Given a set of spatially-close link pairs, assign spatially-close links to the same risk group, while using the minimum number of such groups
R-tree for detecting close links

- grid rectangle
- network link segment
- minimum bounding rectangle
Risk-group algorithm

- Auxiliary graph for representing spatially-close links, with each auxiliary node representing a link
- Links at distance less than $\Delta$ have connected auxiliary nodes
- A maximal clique in the auxiliary graph represents a risk group
The dynamics of risk
Disaster dynamics

- Disasters tend to display spatiotemporal characteristics, and consequently link availabilities may vary in time.

- Connection availability of certain traffic must be guaranteed at (almost) all times, even under disasters.

- When the spatiotemporal impact of disasters (such as the path of a hurricane) can be predicted, preventive actions can be taken.
Risk profile

- A grid-based risk profile, where each grid rectangle $g$ contains an availability value representing the probability that $g$ is free from failure during a specific time period.
The availability of a link is computed as the product of the availability values of all grid rectangles it crosses.

The availability of a path is the product of the availability values of its links.
Spatiotemporal resilience [1]

Given availability values per time slot and for each link the time slots it takes to traverse that link, find an s-d path with maximum availability in time frame $[t_{\text{start}}, t_{\text{end}}]$.

Auxiliary graph

- Layers represent (the nodes at) different time slots
- The most risk-averse path from $s$ to node $d$ is obtained via a shortest path algorithm, using as weights the $-\log$ of the link availabilities

Vertical links only if waiting is allowed
How to get realistic risk numbers?
Advanced network risk model [1]

• Given is a finite set of disasters $D$, each with its own disaster area and probabilities $P(d)$ for all $d \in D$

• Assume exactly one disaster occurs: $\sum_{d \in D} P(d) = 1$

• Deterministic model: all links in disaster area fail

• Obtaining a set of disasters:
  – Monte Carlo
  – Disaster history: last $k$ disasters
  – Representative disaster scenarios

Failure states

• $E$ denotes the set of links

• A failure state $\mathbf{s}$ is defined as a set $\mathbf{s} \subseteq E$, where $\mathbf{e} \in \mathbf{s}$ if and only if link $\mathbf{e}$ is down

• Let $\mathbf{S}$ be the random value indicating the failure state after the disaster and let $\mathbf{S}(\mathbf{d})$ be the failure state after disaster $\mathbf{d} \in \mathbf{D}$

• Typically $|\mathbf{S}[\mathbf{D}]| \ll |\mathbf{D}|$
Vulnerability metric distribution

- Distribution of a vulnerability metric after a (random) disaster
- Can be used to derive worst-case or expected values
- Example metric – Average Two-Terminal Reliability (ATTR):
  - Amount of connected node pairs / total amount of node pairs
Computing the ATTR

• First, compute probability of each failure state $P(S = s)$:
  1. $\forall d \in D$, compute $S(d)$
  2. $\forall s \in S[D]$, store $S^{-1}(s) = \{d \in D | S(d) = s\}$
  3. $\forall s \in S$, $P(S = s) = \sum_{d \in S^{-1}(s)} P(d)$

• Then, only compute ATTR once per possible failure state:
  1. $\forall s \in S[D]$, compute $ATTR(s)$
  2. $\forall a \in ATTR[S[D]]$, store $\{s \in S[D] | ATTR(s) = a\}$
  3. $\forall a \in \mathbb{R}$, $P(ATTR = a) = \sum_{s \in S[D] | ATTR(s) = a} P(S = s)$
Earthquake example

• Two Japanese networks (JGN2plus-Japan of 11 nodes, 10 links, and Sinet of 47 nodes, 49 links)

• All links are assumed to be straight line segments

• J-SHIS earthquake scenarios (2016 dataset of 655 scenarios for 189 fault segments). The JMA seismic intensity threshold was set to 5.5

• ATTR as vulnerability metric
Visualization
Recover in time!
Disaster recovery

• Short term:
  – Reroute traffic **around** disaster area
  – Majority of connections restored

• Long term:
  – Repair and replace affected components
  – Network connectivity restored

Source: https://commons.wikimedia.org/wiki/File:Broken_ethernet_cable.jpg
Disaster repair
(2011 Japan earthquake, NTT)
Temporary emergency nodes

• Temporarily take over network functions
• Quickly installed
• Currently in development/use: e.g. MDRUs, COWs, COLTs, RATs, …

• New problem:
  – Where should we place these nodes?

Source: http://mdru.org/index.php/2-uncategorised/2-about-mdru
Circumstances after a disaster

- Lack of resources
- Lack of information
- Chaos
- Quick decisions required
- Computing optimal node positions is (often) NP-hard
- Short-term recovery strategies needed
Novel approach

• Choose (general) strategy **beforehand**
• Execute directly after disaster

• Our contribution [1]:
  – Framework for evaluating **short-term** recovery strategies

Evaluation framework

Network Topology
Recovery Strategies
Terrain Analysis
Representative Disasters

Network Operator
External Experts

Evaluation Framework
Choose + Prepare Strategy
Disaster Event
Execute Strategy
Strategy evaluation

- Pick one or more (survivability) metrics
- Evaluate strategy to a large set of representative disasters
- Prioritize early effects
Case study

• Incoming hurricane
  – Track prediction by NHC
  – Actual track not completely known

• Goals:
  – Select and prepare suitable strategy
  – Gather appropriate amount of emergency equipment
Disaster set

• Large number of randomly generated realizations of hurricane tracks and affected regions
• Based on NHC track prediction and historical deviation
• Assign importance/probability to each disaster
Evaluation

• Group disasters with the same outcome
• For each recovery strategy
  – For each disaster (group)
    • Compute effect of strategy after disaster
  – Combine results
• Compare results
Effect of a strategy after a disaster

• K nodes selected to replace
• Different replacement times
• K+1 different network states:
  – $G_1, G_2, G_3, \ldots, G_{K+1}$
  – At times $0 = t_1, t_2, t_3, t_4, \ldots, t_{K+1}$
• Early impact more important than late impact
  – Weight factor
Expected Weighted Connectivity (ATTR)

<table>
<thead>
<tr>
<th></th>
<th>K=1</th>
<th>K=2</th>
<th>K=3</th>
<th>K=6</th>
<th>K=10</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Optimal</strong></td>
<td>0.067</td>
<td>0.098</td>
<td>0.127</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Greedy</strong></td>
<td>0.067</td>
<td>0.095</td>
<td>0.122</td>
<td>0.180</td>
<td>0.215</td>
</tr>
<tr>
<td><strong>Weight/Cost</strong></td>
<td>0.022</td>
<td>0.043</td>
<td>0.063</td>
<td>0.134</td>
<td>0.191</td>
</tr>
<tr>
<td><strong>Neighbors/Cost</strong></td>
<td>0.035</td>
<td>0.064</td>
<td>0.083</td>
<td>0.128</td>
<td>0.189</td>
</tr>
<tr>
<td><strong>Random</strong></td>
<td>0.006</td>
<td>0.013</td>
<td>0.020</td>
<td>0.041</td>
<td>0.082</td>
</tr>
</tbody>
</table>

Greedy Wins – in this case!
Conclusion

• Network elements are bound to fail and hence call for resiliency measures

• Both the likelihood of disasters and their impact on society are increasing, and demand a spatiotemporal perspective to network resilience engineering

• Spatiotemporal resilience also relies on monitoring, machine learning, BCM strategies, etc., and consequently provides many research opportunities…
Further reading (1/3)


Further reading (2/3)


Further reading (3/3)

