Modelling and Design of the Resilient and Survivable Future Internet under Challenges

Egemen K. Çetinkaya and James P.G. Sterbenz

Department of Electrical Engineering & Computer Science
Information Technology & Telecommunications Research Center
The University of Kansas

ekc@ittc.ku.edu

http://www.ittc.ku.edu/~ekc
http://wiki.ittc.ku.edu/resilinets
Abstract

Communication networks, in particular the Internet, face a variety of challenges that can disrupt our daily lives resulting in human life and financial losses in the worst cases. We define challenges as external events that trigger faults that eventually result in service failures. Understanding these challenges accordingly is essential for improvement of the current networks and for designing Future Internet architectures. We surveyed a wide spectrum of challenges and categorized them. Next, we studied challenges and their impacts on physical and logical network topologies. Our initial results show that different layers of networks demonstrate varying performance and it is crucial to model and study challenges accordingly. Ultimately, we aim to design topologies that are resilient to communication network challenges.
Network Challenge Framework

Outline

• Introduction and motivation
• Resilience disciplines
• Challenge definition and examples
• Challenge taxonomy
• Challenge modelling
Introduction and Motivation

• Introduction and motivation
• Resilience disciplines
• Challenge definition and examples
• Challenge taxonomy
• Challenge modelling
Network Challenge Framework

Introduction and Motivation

• Networks face challenges that are costly
• Understanding the network behaviour is crucial
  – Future Internet architectures and design of new protocols
  – network engineering of existing networks
• Other motivation:
  – most effective disruptions to dark networks
  – fault analysis of electronics circuit boards
  – transportation optimisations
Network Challenge Framework
Resilience Disciplines

- Introduction and motivation
- Resilience disciplines
- Challenge definition and examples
- Challenge taxonomy
- Challenge modelling
Resilience Disciplines

Sub-Disciplines: Challenge Tolerance

- **Survivability**: many \( \vee \) targetted failures
- **Fault Tolerance**: (few \( \land \) random)
- **Traffic Tolerance**: legitimate, flash crowd, attack, DDoS

- **Disruption Tolerance**: environmental
  - delay, mobility, connectivity
  - energy

- **Robustness Complexity**
  - Trustworthiness
    - Dependability: reliability, maintainability, safety
    - Availability: integrity
    - Confidentiality: confidentiality
    - Auditable: auditability
    - Authoritative: authorisability
    - Authenticity: authenticity
  - Security: AAA
  - Performability: QoS measures
  - Maintainability: safety
  - Safety: QoS measures
Resilience Disciplines
Sub-Disciplines: Challenge Tolerance

• Survivability against attack and large-scale disasters
  - tolerate many and correlated failures
  - fault tolerance: tolerate one (or several) random failures
    • subset of survivability sub-discipline

• Traffic tolerance
  - DDoS attacks
  - legitimate traffic such as flash crowds

• Disruption tolerance
  - tolerate environmental challenges
  - mobility, weak/episodic connectivity, unpredictably long delay
Network Challenge Framework

Challenge Definitions and Examples

- Introduction and motivation
- Resilience disciplines
- Challenge definition and examples
- Challenge taxonomy
- Challenge modelling
Challenges

Definition

• Challenge: adverse event or condition
  - unintentional misconfiguration or operational mistakes
  - malicious attacks
  - large-scale natural disasters
  - environmental challenges
    • mobility
    • weak and episodic channels (typically wireless)
    • unpredictably long delay
  - unusual but legitimate traffic (e.g. flash crowd)
  - dependent failures
    • interdependent infrastructure
    • service failure at a lower level
    • cascading failure
  - social, political, economical, and business factors
### Challenge Properties

**Spatial and Temporal Characteristics**

<table>
<thead>
<tr>
<th>Challenge examples</th>
<th>Spatial Region</th>
<th>Temporal Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>geographic</td>
<td>impact</td>
</tr>
<tr>
<td>earthquake</td>
<td>100s km²</td>
<td>100s km²</td>
</tr>
<tr>
<td>fire</td>
<td>100s m²</td>
<td>10s km²</td>
</tr>
<tr>
<td>hurricane</td>
<td>100s km²</td>
<td>100s km²</td>
</tr>
<tr>
<td>solar storm</td>
<td>10000s km²</td>
<td>10000s km²</td>
</tr>
<tr>
<td>misconfiguration</td>
<td>node</td>
<td>global</td>
</tr>
<tr>
<td>malicious attack</td>
<td>node</td>
<td>global</td>
</tr>
<tr>
<td>terrorism</td>
<td>100s m²</td>
<td>global</td>
</tr>
<tr>
<td>policy related</td>
<td>N/A</td>
<td>global</td>
</tr>
<tr>
<td>depeering</td>
<td>N/A</td>
<td>global</td>
</tr>
<tr>
<td>pandemic</td>
<td>global</td>
<td>global</td>
</tr>
<tr>
<td>power blackout</td>
<td>100s km²</td>
<td>regional</td>
</tr>
<tr>
<td>lower level service failures</td>
<td>node/link</td>
<td>regional</td>
</tr>
</tbody>
</table>
Definitions

Challenge $\rightarrow$ Fault $\rightarrow$ Error $\rightarrow$ Failure

- **Challenge**
  - adverse event or condition that impacts normal operation
  - external event that triggers a fault

- **Fault**
  - property of a system based on its design

- **Error**
  - stochastic event in either space (system) or time
  - manifestation of a fault

- **Service failure**
  - deviation of delivered service from service specification

[Wiki 2006, SHCJ RSS 2010, ALRL 2004]
Fault → Error → Failure Chain

Challenges and ResiliNets Strategy

Disasters: natural, man-made
Non-malicious: ops., traffic, accidents
Malicious attacks
Unusual traffic: flash crowds
Socio-political and economical factors
Dependent failures
Environmental: mobility, connectivity, delay

Challenges

Detect

Defend

Active Faults

System Operation

Errors

Dormant Faults

Detect

Defend

Diagnose Refine

Errors passed on to operational state

[Wiki 2006, SHCJ RSS 2010]
Network Challenge Framework

Challenge Taxonomy

• Introduction and motivation
• Resilience disciplines
• Challenge definition and examples
• Challenge taxonomy
• Challenge modelling
Challenge Taxonomy
Overview

• Classification and taxonomy of challenges
  - based on fault taxonomy
    • [ALRL 2004] and IFIP 10.4 related publications

• Elementary challenge classes
  - elementary orthogonal classification within fault groups

phenomenological cause
  target
  objective
  intent
  capability
dimension
domain
scope
significance
persistence
repetition
**Challenge Taxonomy**

**Elementary Challenge Classes**

- Elementary challenge classes
  - phenomenological cause
  - target
  - objective
  - intent
  - capability
  - dimension

- Based on 10.4 fault taxonomy
  - some correspond directly; some new
  - not all binary choices, some multiple levels
  - not all combinations possible
    - e.g. natural challenges (phenom.) can’t be malicious (objective)
## Challenge Taxonomy

### Preliminary Correlation Matrix

<table>
<thead>
<tr>
<th>Challenge examples</th>
<th>intent</th>
<th>scope</th>
<th>domain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>non-malicious</td>
<td>malicious</td>
<td>nodes</td>
</tr>
<tr>
<td>natural component failures</td>
<td>×</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>misconfiguration</td>
<td>×</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>cable cuts</td>
<td>×</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>jammers</td>
<td></td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>interference</td>
<td>×</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>weather precipitation</td>
<td>×</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>attacks against critical inf.</td>
<td>×</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>natural disasters</td>
<td>×</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>pandemic</td>
<td>×</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>nationwide Internet outage</td>
<td>×</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>power failure</td>
<td>×</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>EMP weapon</td>
<td></td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>coronal mass ejection</td>
<td>×</td>
<td></td>
<td>×</td>
</tr>
</tbody>
</table>
Network Challenge Framework

Challenge Modelling

- Introduction and motivation
- Resilience disciplines
- Challenge definition and examples
- Challenge taxonomy
- Challenge modelling
Simulation Framework
KU-CSM ns-3 Model

• **Input**
  - user defined network and challenge specification

• **Output**
  - network performance under specified challenges
Simulation Framework

Challenge Types

- Challenge types
  - node or link down
    - random or attack (deg, betweenness, …)
  - area based challenge
    - $n$-sided polygon: $(x_0, y_0), \ldots, (x_{n-1}, y_{n-1})$
    - circle centered at $(x_0, y_0)$ with radius $r$
  - wireless link attenuation or jamming

- Challenge characteristics
  - type (e.g. wired/wireless)
  - class (e.g. important peering node)
  - dynamic: interval $(t_i, t_j)$, trajectory
Multilevel Challenge Analysis

Sprint Example: Physical vs. L3 PoPs

- Combined plots for physical and logical topologies
  - circle with radius $r$ or $n$-sided polygon simulations
  - challenges evolve spatially or temporally [CBDSS 2011]
Simulation Results
Analysis of Logical vs. Physical Topologies

- Sprint fiber routes with MPLS nodes as source
- Southcentral challenge not impacting logical topology
- Logical: 100% vs. physical: 98 -> 91 -> 86% PDR
References

- [Wiki 2006]  https://wiki.ittc.ku.edu/resilinets
End of Foils
Backup Foils

Taxonomy
Challenge Taxonomy
Overview

- Classification and taxonomy of challenges
  - based on fault taxonomy
    - [ALRL 2004] and IFIP 10.4 related publications
- Elementary challenge classes
  - elementary orthogonal classification within fault groups

<table>
<thead>
<tr>
<th>phenomenological cause</th>
<th>challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>dimension</td>
</tr>
<tr>
<td>objective</td>
<td>scope</td>
</tr>
<tr>
<td>intent</td>
<td>significance</td>
</tr>
<tr>
<td>capability</td>
<td>persistence</td>
</tr>
<tr>
<td>repetition</td>
<td></td>
</tr>
</tbody>
</table>
Challenge Taxonomy
Elementary Challenge Classes

- Elementary challenge classes
  - phenomenological cause
  - target
  - objective
  - intent
  - capability
  - dimension

- Based on 10.4 fault taxonomy
  - some correspond directly; some new
  - not all binary choices, some multiple levels
  - not all combinations possible
    * e.g. natural challenges (phenom.) can’t be malicious (objective)
Phenomenological cause

- **Natural challenges**
  - terrestrial e.g. earthquakes
  - meteorological e.g. hurricanes and ice storms
  - cosmological e.g. CMEs (coronal mass ejections)

- **Human challenges**
  - social e.g. recreational cracker
  - political and ethnic e.g. political unrest
  - business and economic e.g. depeering
  - Terrorism e.g. 9/11 and London bombings

- **Dependencies**
Challenge Taxonomy

Phenomenological Cause: Dependencies

Phenomenological cause

- **Natural challenges**
- **Human challenges**
- **Dependency**
  - *interdependent infrastructure* e.g. power grid failure on net
  - *lower level failure* challenging higher layers of infrastructure
    - e.g. cable cuts, Georgian woman cutting Armenian Internet
  - *cascading failure* propagating at a given level
    - e.g. incorrect BGP prefix propagation
Challenge Taxonomy

Target

- **Direct**
  - challenge directed at the infrastructure that may fail
  - e.g. sabotage on cables

- **Collateral**
  - challenge directed at interdependent infrastructure
  - e.g. 9/11 was not targetted at Internet or PSTN
Objective

- **Malicious**
  - introduced by human with intent to harm system
  - may be automated (e.g. Botnet)

- **Selfish**
  - introduced with selfish intent (e.g. not coöperating)

- **Non-malicious**
  - introduced without malicious objective
  - include all natural challenges
  - include human deliberate incompetence challenges
  - include human non-deliberate accidental challenges
Intent

- *Deliberate faults*
  - result of a harmful decision
- *Non-deliberate faults*
  - introduced without awareness
  - include mistakes
Challenge Taxonomy
Capability

- **Accidental challenges**
  - introduced inadvertently

- **Incompetence challenges**
  - from lack of professional competence by authorised humans
  - inadequacy of development or deployment organisation
Challenge Taxonomy

Dimension

- **Hardware failures**
  - target hardware
  - network components and physical links

- **Software failures**
  - target software
  - operating systems and protocol software

- **Protocol failures**
  - target protocol operation and signalling

- **Traffic**
  - overload of network by legitimate traffic
  - malicious attack (e.g. DDoS)
Domain

- **Wired challenges**
  - target wired network infrastructure
  - optical and copper links and related components

- **Wireless challenges**
  - target wireless infrastructure
  - wireless medium and related components
  - e.g. jamming
Challenge Taxonomy

Scope

- **Node challenges**
  - target nodes: switches, routers, and other components

- **Link challenges**
  - target wired links or wireless spectrum

- **Area challenges** affect nodes and links
  - *fixed* challenge over a given area
  - *evolving* challenge moving or changing in area
Significance

related to ATIS T1A1 extent in (U,D,E) triple

- **Minor challenges**
  - small in scope or intended consequences

- **Major challenges**
  - large in scope or intended consequences
  - include large areas and attacks against critical subsystems

- **Catastrophic challenges**
  - catastrophic in scope or intended consequences
  - include very large areas
  - include attacks against many critical subsystems
Persistence

- **Persistent challenges** from an adverse condition
  - *short-lived challenges*
  - *long-lived challenges*
  - remediation important during challenge
  - recovery after adverse condition ends

- **Transient challenges** from adverse events
  - single event challenges
  - remediation needed if physical infrastructure destroyed
  - recovery most important after challenge event
Repetition

- **Single challenge**
  - single instance of a given challenge

- **Repeated challenge**
  - repeated instance of a given challenge

- **Adaptive challenge**
  - repeated instance of a challenge that adapts to failures
Backup Foils
KU-CSM
Challenge Evaluation
Simulation-based Models

• Graph-based
  - primarily involved random networks
  - investigates node degree and betweenness

• Large-scale geographic simulation models
  - challenge areas modelled as: polygon, circle, line
  - essential for physical topologies

• Attack simulations
  - useful for attacks on logical topologies

• Wireless disruption simulations
  - not widely studied
Simulation Framework
KU-CSM ns-3 Model

- **Input**
  - user defined network and challenge specification
- **Output**
  - network performance under specified challenges

26 April 2012
Simulation Framework

Challenge Types

- Challenge types
  - node or link down
    - random or attack (deg, betweenness, …)
  - area based challenge
    - $n$-sided polygon: $(x_0, y_0), \ldots, (x_{n-1}, y_{n-1})$
    - circle centered at $(x_0, y_0)$ with radius $r$
  - wireless link attenuation or jamming

- Challenge characteristics
  - type (e.g. wired/wireless)
  - class (e.g. important peering node)
  - dynamic: interval $(t_i, t_j)$, trajectory
Simulation Framework

Implementation of Challenge Models

- Network performance modelling is non-trivial
- Non-malicious challenges
  - to model random node and links failures
  - set-down nodes and links for the challenge duration
- Malicious attacks
  - set-down critical nodes and links for the challenge duration
- Large-scale disasters
  - to model natural or man-made large-scale disasters
  - n-sided polygon and circular areas modelled
  - challenge area can evolve spatially or temporally
• Wireless challenges
  - have not been studied much
  - new propagation model with mobility and range of influence
    • loss based on closest distance from the center of impairment
    • to the line segment between two nodes
  - jammers send high power signal at a high rate
Simulation Results
Sample Topologies

• Sample topologies
  – Sprint inferred via Rocketfuel
  – synthetic 1
  – synthetic 2

• Synthetic topologies
  – generated via KU-LocGen
  – keeps the node positions
  – connectivity via Waxman-model
  – cost-constrained
## Simulation Results
Characteristics of Sample Networks

<table>
<thead>
<tr>
<th>Topology</th>
<th>Sprint inferred</th>
<th>Synthetic 1</th>
<th>Synthetic 2</th>
</tr>
</thead>
<tbody>
<tr>
<td># nodes</td>
<td>27</td>
<td>27</td>
<td>27</td>
</tr>
<tr>
<td># links</td>
<td>68</td>
<td>74</td>
<td>68</td>
</tr>
<tr>
<td>Max. degree</td>
<td>12</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>Avg. degree</td>
<td>5.04</td>
<td>5.5</td>
<td>5.04</td>
</tr>
<tr>
<td>Clus. coefficient</td>
<td>0.43</td>
<td>0.29</td>
<td>0.38</td>
</tr>
<tr>
<td>Net. Diameter</td>
<td>6</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Avg. hopcount</td>
<td>2.44</td>
<td>2.2</td>
<td>2.9</td>
</tr>
<tr>
<td>Node betweenness max/min/avg.</td>
<td>144/28/72</td>
<td>76/2/36.8</td>
<td>302/2/269.9</td>
</tr>
<tr>
<td>Link betweenness max/min/avg.</td>
<td>72/2/12.6</td>
<td>31/1/10.5</td>
<td>140/1/14.9</td>
</tr>
</tbody>
</table>
Simulation Results

Simulation Parameters

• P2P links with 10 Mb/s and 2 ms delay
• Routing: Dijkstra shortest path first algorithm
• Application traffic: 40 kb/s
  – between every pair of nodes
• Packet size: 1000 B
• Random cases were averaged over 100 runs
• PDR for performance evaluation on sample topologies
Simulation Results
Link Failure Analysis

- Analysis of up to 10 link failures
- Link attacks based on betweenness on links
- Attacks reduce PDR more compared to random cases
Simulation Results
Node Failure Analysis

• Analysis of up to 10 node failures
• Attacks based on degree of connectivity, betweenness
• Node attacks/failures impact more compared to links
Simulation Results
Random Node and Link Failure Analysis

- Analysis of all node and link failures
- Node failures impact more compared to links
- synthetic1 > synthetic2 > inferred
Simulation Results
Large-scale Network Failure Analysis
Simulation Results
Large-scale Network Failure Analysis

• Topologies used:
  - Rocketfuel-inferred Sprint topologies
  - Sprint long-haul fiber routes and Sprint MPLS PoPs

• Area-based challenges modelling:
  - temporally evolving circle (e.g. EMP Bomb)
  - temporally moving circle (e.g. hurricane)
  - temporally evolving polygon (e.g. power blackout)

• Characteristics of the logical and physical identical
  - similar curves
    • depends on number of nodes and link in the challenge area
Simulation Results

Analysis of Logical vs. Physical Topologies

- Sprint fiber routes with MPLS nodes as source
- Southcentral challenge not impacting logical topology
- logical: 100% vs. physical: 98 > 91 > 86% PDR
Simulation Results

Wireless Domain Challenges

- jammer [-100,0]
- receiver [0,0]
- sender [300,0]
- impairment sweeps
- mobility pattern of jammer results attacks or failures