Future Internet Resilience
Summary of Networking Research at The University of Kansas ITTC

James P.G. Sterbenz

Department of Electrical Engineering & Computer Science
Information Assurance, Communication & Network System Labs
Information Technology & Telecommunications Research Center
The University of Kansas

jgps@ittc.ku.edu
http://www.ittc.ku.edu/~jgps
http://wiki.ittc.ku.edu/resilinets

10 June 2010
Major related research themes

- future Internet architecture and infrastructure
- resilient and survivable networks
- information assurance and security
- disruptive and novel communication paradigms
Collaborators

- regional: K-State, UMKC, UNL, ...
- national: Rutgers, Penn State, CMU, ORNL, ...
- international: U. Lancaster UK, ETH Zürich, TU-Munich, ...

Funding

- NSF FIND, GENI, ...
- DoD DARPA, CTEIP, ...
- EU FP6 SAC, FP7 FIRE
- Industry: Sprint, ...
Resilient Networks

Motivation

• Increasing reliance on network infrastructure
  ⇒ Increasingly severe consequences of disruption
  ⇒ Increasing attractiveness as target from bad guys
• Internet is *critical infrastructure*
  • interdependent with other CI, e.g. power grid
Resilient Networks
Resilience Definition

- **Resilience**
  - provide and maintain acceptable service
  - in the face of faults and challenges to normal operation

- **Challenges**
  - faults
  - unintentional misconfiguration or operational mistakes
  - large scale disasters (natural and human-made)
  - malicious attacks from intelligent adversaries
  - environmental challenges (wireless, mobility, delay)
  - unusual but legitimate traffic
  - service failure at a lower level
Resilience Scope
Relationship to Other Disciplines

Challenge Tolerance
Survivability
- many ∨ targetted failures
Fault Tolerance
- (few ∧ random)
Traffic Tolerance
- legitimate, flash crowd, attack, DDoS

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

Robustness Complexity

Trustworthiness
Dependability
- reliability, maintainability, safety

Availability
- confidentiality, nonrepudiability

Integrity
- auditability, authorisability, authenticity

AAA
- authenticity, authorisability

Performability
- QoS measures

Security
- confidentiality, nonrepudiability

Challenge Tolerance
Survivability
Fault Tolerance
Traffic Tolerance
Disruption Tolerance
- environmental
Robustness Complexity

Dependability
- reliability, maintainability, safety

Availability
- confidentiality, nonrepudiability

Integrity
- auditability, authorisability, authenticity

AAA
- authenticity, authorisability

Performability
- QoS measures
Resilience Architecture

ResiliNets Strategy: $D^2R^2 + DR$

- **Real time control loop:** $D^2R^2$
  - defend
    - passive
    - active
  - detect
  - remediate
  - recover

- **Background loop:** $DR$
  - diagnose
  - refine

[ComNet 2010]
Resilience Architecture

ResiliNets Principles

- Prerequisites: to understand and define resilience
- Tradeoffs: recognise and organise complexity
- Enablers: architecture and mechanisms for resilience
- Behaviour: require significant complexity to operate
Resilience Architecture
Multilevel Resilience and Cross-Layering

- ResiliNets Cube
  - multilevel
    - protocol layers
    - planes
    - mechanisms
- D^2R^2+DR strategy
  - D^2R^2 control plane
  - DR mgt. plane
- Cross-layering
  - knobs and dials are metrics
  - K, D ⊆ N u P
Resilience Quantification
State Space: Operational Resilience

- Operational resilience
  - minimal degradation
  - in the face of challenges
- Resilience state
  - remains in normal operation
Resilience Quantification
State Space: Service Resilience

- Service resilience
  - acceptable service
  - given degraded operation
- Resilience state
  - remains in acceptable service
- Resilience
  - $\mathbb{R} = \text{area under trajectory}$
  - for particular scenario
  - resilience $\mathbb{R}$ over all scenarios
Resilience Quantification
$D^2R^2 + DR$ Relationship to State Space

- **Real time control loop:** $D^2R^2$
  - **defend** keeps toward origin
    - passive
    - active
  - detect when leaves
  - remediate pushes back
  - recover back to origin
- **Background loop:** $DR$
  - diagnose
  - refine tightens trajectory
Resilience Evaluation

Topology Generation: KU-LoCGen

- Generation of realistic topologies
- Multilevel hierarchy
  - level 1: represents (tier 1) backbone
  - level 2: represents access networks around a backbone PoP
  - level 3: represents subscriber nodes
- Constrained generation
  - geographic node location (infrastructure or population)
  - constrained link location (based on exiting fiber runs)
  - constrained cost (fixed + variable cost)
  - graph-theoretic constraints for resilient diversity
Resilience Evaluation
Evaluating Challenges in State Space

- Topology generation
  - use KU-LoCGen
- Challenge simulation
  - random failures
  - intelligent attacks
    - degree, betweenness, etc.
  - large scale disasters
    - hurricanes, blackouts
- Example
  - resilience of alternatives based on Sprint PoPs
• **KU-CSM Challenge Simulation Module**
  - **challenge specification** describes challenge scenario
  - **network coordinates** provide node geo-locations
  - **adjacency matrix** specifies link connectivity
  - **input to conventional** **ns-3 simulation run**
  - generates trace to **plot results**

**KU-LoCGen**
Resilience Evaluation
KU-CSM Challenge Simulation

- Example: evolving area-based challenge example
  - circle moving from Orlando to NY
- Performability analysis: packet delivery ratio
  - PDR varies with # links nodes down
Enabling Future Internet Research

GpENI Overview

- Great Plains Environment for Network Innovation
  - part of NSF GENI program
  - affiliated with EU FP7 FIRE programme / ResumeNet project
- Programmable network infrastructure (L1–7)
  - Midwest US optical backbone
  - International testbed
- Conduct experiments in:
  - future Internet architectures
  - resilience and survivability
  - cross-evaluation with analytical- and simulation-based eval.

<table>
<thead>
<tr>
<th>GpENI Layer</th>
<th>Programmability</th>
</tr>
</thead>
<tbody>
<tr>
<td>experiment</td>
<td>Gush, Raven</td>
</tr>
<tr>
<td>application</td>
<td>PlanetLab</td>
</tr>
<tr>
<td>end-to-end</td>
<td>Quagga, XОРP, Click</td>
</tr>
<tr>
<td>router</td>
<td>VINI</td>
</tr>
<tr>
<td>topology</td>
<td>DCN</td>
</tr>
<tr>
<td>VLAN</td>
<td>site-specific</td>
</tr>
<tr>
<td>lightpath</td>
<td>[TridentCom 2010]</td>
</tr>
</tbody>
</table>
Enabling Future Internet Research
GpENI Midwest Optical Node Cluster

- GpENI cluster
  - 5–10 PCs
    - GpENI mgt.
    - L4: PlanetLab
    - L3: prog. routers
- GbE switch
  - arbitrary site interconnection
  - L2: GpENI/GENI VLAN
  - SNMP cluster monitoring
- Ciena optical switch
  - L1 GpENI interconnection
Enabling Future Internet Research
GpENI Midwest Optical Backbone

- Physical topology
  - multiwavelength optical backbone
  - current or imminent deployment
  - 4 universities in 3 states
  - 1 switch/year with current funding
Enabling Future Internet Research
GpENI European Expansion

- European GpENI partners
  - 13 nations
  - 24 research institutions
  - ~120 nodes
  - more under discussion
Enabling Future Internet Research
GpENI Asian Expansion

- Asian GpENI partners
  - 3 nations
  - 5 research institutions
  - 25 nodes
  - more under discussion
ITTC Networking Research

Selected Project Examples

- Weather disruption-tolerant networking (Sterbenz)
- Highly-dynamic airborne networking (Sterbenz)
- Information security and privacy (Luo)
- SDRs and cognitive networking (Minden, Evans)
- Sensor networking (Frost)
WDTN Project Overview

• Mesh architecture
  – high degree of connectivity
  – alternate diverse paths
    • severely attenuated mm wave
    • alternate mm, lower-freq. RF
    • fiber bypass (competitor)

• Solution [INFOCOM 2009]
  – reroute before link failures they occur
  – P-WARP predictive routing
    • image radar to predict weather
  – XL-OSPF instantaneously reactive routing
    • cross-layered with BER estimation
Airborne Networking Project

Scenario

- **Very high relative velocity**
  - Mach 7 \( \approx 10 \) s contact
  - dynamic topology
- **Communication channel**
  - limited spectrum
  - asymmetric links
    - data down omni
    - C&C up directional
- **Multihop**
  - among TAs
  - through relay nodes
Airborne Network Project
Protocol Stack and Interoperability

- **AeroTP**: TCP-friendly transport
- **AeroNP**: IP-compatible forwarding
- **AeroRP**: routing

[HMI apps] gNET

[TA peripherals] [MILCOM 2008]
InfoSec and Privacy Projects
[Bo Luo PI]

- **CAT**: A node-failure-resilient anonymous communication protocol through commutative path hopping [INFOCOM 2010]
  - protect the identity/privacy of communication participants
  - group-based path probing & commutative path hopping: resilient to relay node failures

- **Secure in-network operations for smart grids**
  - in-network operations:
    distribute operations (e.g. aggregation) into smart meters
  - Secure operations:
    perform operations without revealing the data, using applied crypto methods
**SDR and Cognitive Radio Projects**

[Gary Minden and Joseph Evans PIs]

- **KUAR**: KU agile radio
  - experimental system: wireless networking & radio research
  - 5.8 GHz UNII band; independent 30MHZ tx/rx signal paths,
  - signal processing is entirely in an FPGA and GPU

- **Application**
  - sharing radio frequency spectrum with multiple users
  - configure radio software for specific missions
  - adaptation to dynamic RF environment and other users
  - radio network control and resource management

- **Cognitive networking**
  - new dynamic routing algorithms exploiting SDR technologies
SDR and Cognitive Radio Projects

KUAR Diagrams

Software Organisation

ResiliNets Overview
Objective and problem
- KC SmartPort is encouraging development
- transport systems require
  - visibility, accountability, efficiency, security

Transportation security approach
- sensing, communications, and information integration
- integrate sensor information and real-time tracking with... trade data documents to correlate
- expand the ORNL SensorNet technologies
  - to mobile rail network environment
End

Questions?