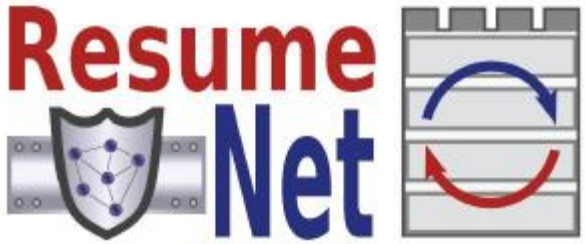


ResumeNet

Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation

http://www.resumenet.eu

Problem statement

- The Internet has become a critical infrastructure – but has it been designed to be one?
- The Internet is vulnerable ...
  - to flaky communication channels (supporting mobility)
  - unintentional misconfiguration
  - large scale (natural) disasters
  - malicious attacks
  - unusual usage and traffic loads
- Needed: A fundamentally new architectural approach towards a resilient Internet

Resilience

- Ability of the system to provide and maintain an acceptable level of service, despite adverse conditions
  - Unintentional misconfiguration
  - Operational mistakes
  - Natural and man-made disasters
  - Malicious attacks
  - Intrinsic challenges (mobility, bad channels, variable delays, …)
  - Foreseen and unforeseen user behavior
- Property of network and application level services

Main objectives and approach

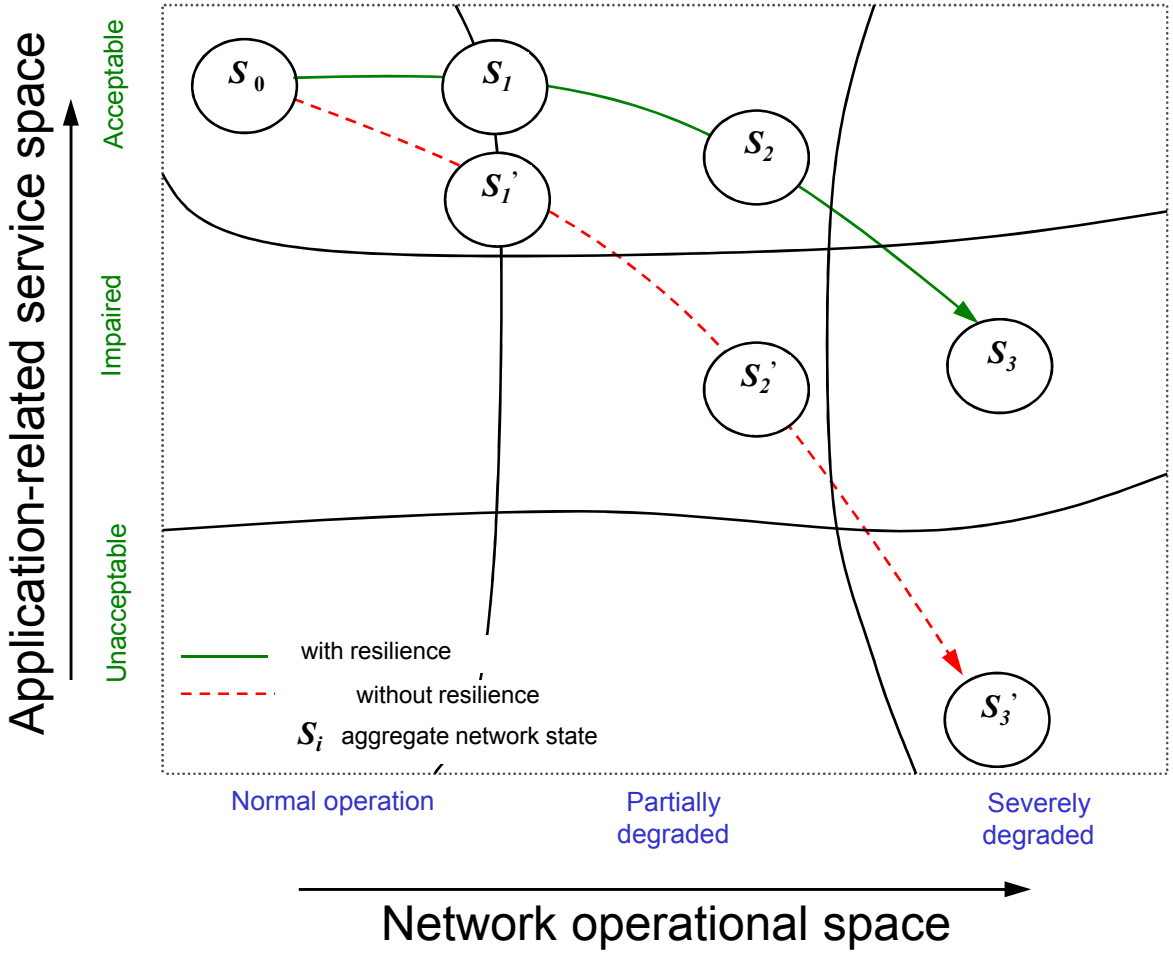
BP3

- To systematically embed resilience into the future Internet
- Three dimensions:
  - Conceptual framework
  - Mechanisms and algorithms for
    - Network resilience (redundancy, topology control, attack detection, ...)
    - Services resilience (overlays, P2P technology, virtualization, ...)
  - Experimentation in testbeds
    - {network, service, failure, resilience mechanism, cross-layer}
- Link with other projects in the Future Internet area

BP3 Adapt content and formatting

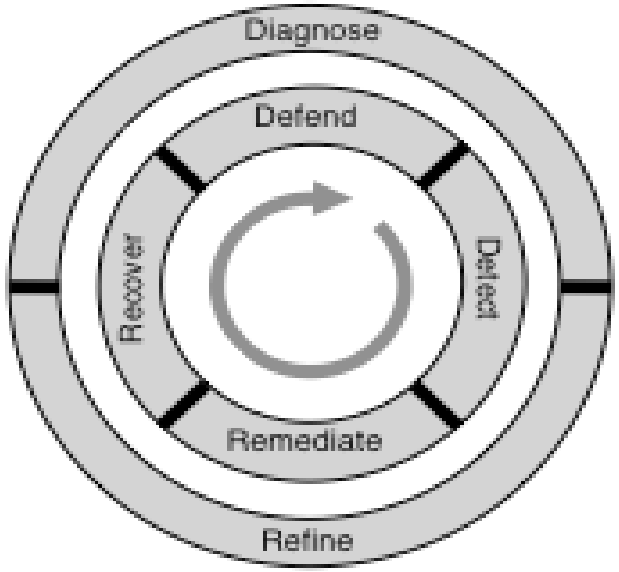
Bernhard Plattner; 23.01.2008

Network and service resilience objectives



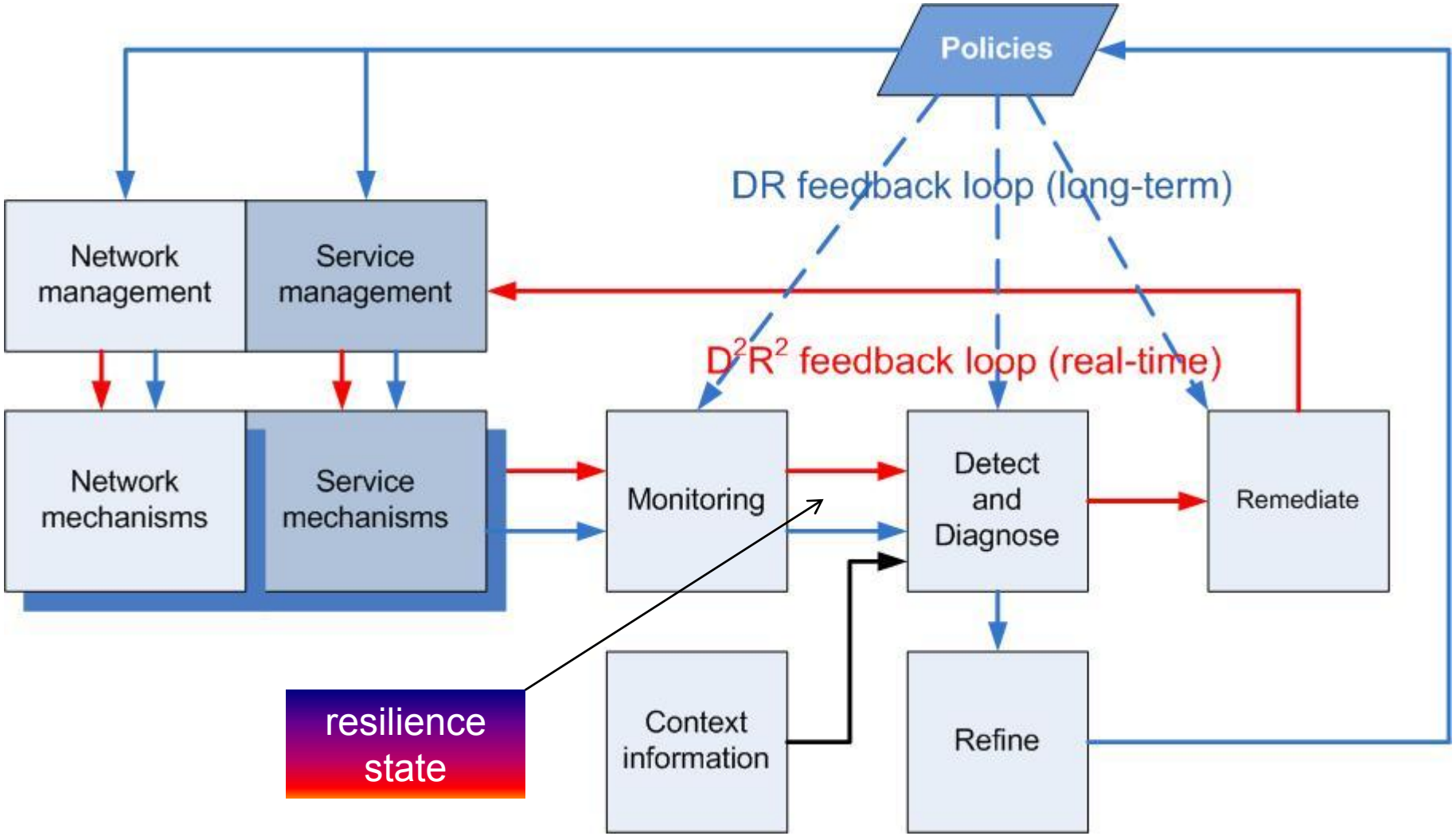
Resilient Networking Strategy - D^2R^2+DR

- Real-time Control Loop
  - Defend (proactively)
  - Detect
  - Remediate (reactively)
  - Recover
- System Enhancement
  - Diagnose
  - Refine



- ResumeNet validates strategy and provides guidelines for practitioners

Network and service resilience architecture



Research questions

- Distributed algorithms implementing this architecture
- Formalize resilience state vector (network/services)
- Find metric for resilience → *grade* of resilience
- Estimator for network/service resilience state
- Two feedback loops: Control-theoretic approach
- Optimization problem: maximize grade of resilience given (resilience state, available mechanisms, context information, user needs)

  ... and others we are not yet aware of

Taxonomy of challenges impairing net/serv

- Component faults
  - Hardware failures (reliability theory)
  - Software faults (systematic)
- Hardware destruction
  - By disaster, terrorist attacks
- Communication environment
  - Mobility, wireless channels
- Human errors
  - Non malicious
  - Misconfiguration
- Malicious attacks
  - DoS, collateral damages
- Unusual but legitimate requests
  - Flash crowds
- Provider failure
  - Exogenous effect

Exemplary challenge characterization

Challenge	Name	Frequency Jammer
Classification	Category	Malicious attack
	Scenario	Wireless communication
Characteristics	Description	The frequency used for communication is jammed by a) constant, b) periodic, c) interactive, d) arbitrary transmissions of the attacker.
	Scope	MAC layer
	Potential Impact	Communication among nodes in the vicinity is prevented or severely degraded
Details	Parameters	Duration of interference, period of jamming signal, output signal strength
	Symptoms	MAC layer protocol violation, disrupted link frames, reduced link bandwidth

Towards an assessment of operational risk

Project organization

- 3-year long STREP, starting 01/09/2008
- Nine partners from 7 countries
  - Seven academic and two industrial partners
  - Visiting researchers from US and Australia affiliated with ULANC
- 6 WPs
  - Concepts and framework
  - Network resilience
  - Service resilience
  - Experimentation / Testbeds
  - Dissemination
  - Management
- Budget: ~3050k€

The ResumeNet Consortium

Eidgenössische Technische Hochschule Zürich	Switzerland
Lancaster University	United Kingdom
Technische Universität München	Germany
France Telecom	France
NEC Europe Ltd	United Kingdom
Universität Passau	Germany
Technical University Delft	Netherlands
Uppsala Universitet	Sweden
Université de Liège	Belgium