

FP7 ResumeNet STREP

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

**Bernhard Plattner, ETH Zurich, Switzerland
Project coordinator**





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



Disclaimer

The statements given here mainly reflect the presenter's opinion and were only superficially discussed in the consortium.

They should not be taken as an official ResumeNet position.

Note: ResumeNet will (hopefully) start on September 1, 2008



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



Main objectives and approach

- 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}



Experimentation in ResumeNet

- Objective: Evaluate the work carried out in the R&D work packages
- Experiments planned
 1. Resilient routing and medium sharing in Wireless Mesh Networks
 - Selfish nodes / broken nodes
 - In-house hybrid wireless mesh test network
 - Experimentation facility provided by the ANA project
 2. Resilient forwarding in opportunistic networks
 - Active and passive attacks against opportunistic forwarding algorithms
 - Failure detection and recovery tests
 - Extension of Uppsala in-house Haggie test bed



Experiments planned (contd.)

1. Service-level resilience evaluation

- Test-bed: VoIP infrastructure (SIP clients, proxies, registrars, AAA, ...)
- P2P routing and virtualization
- Component failures, routing failures, flash crowds, DDoS attacks

2. Resilient smart environments

- Smart spaces, with mobile sensors and actuators
- Policies defining resilience requirements (availability/security/safety)
- Testing the system capability to adapt to threats (dynamic modification of policies)

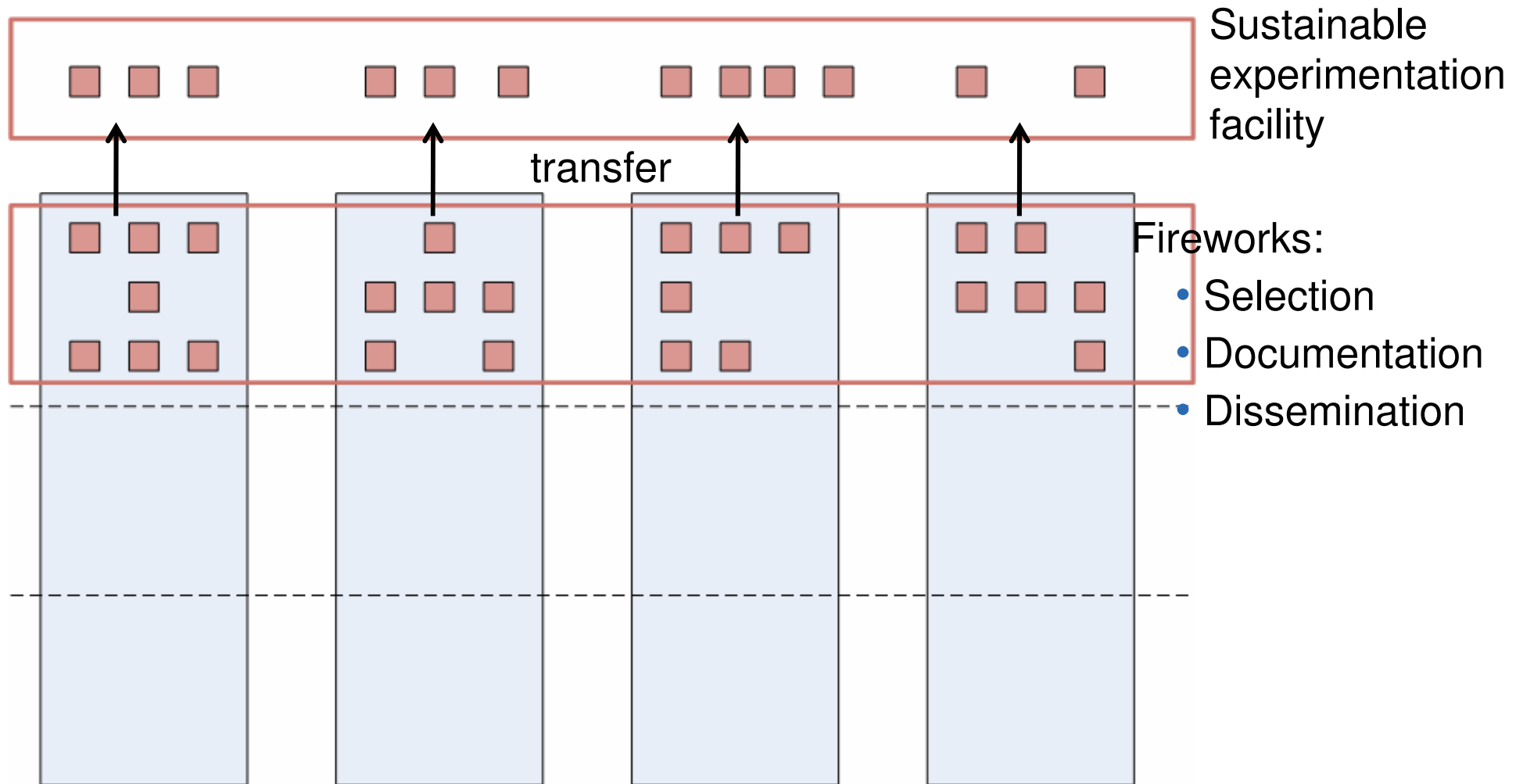
- Experiments are in-house/in-project

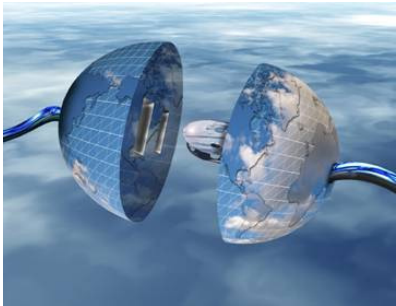


Desired properties of a wireless testbed

- Experimentation with real transmitters/receivers
- Scalability
 - $n=10, 100, 1000$
 - Support variation of node densities → spatial testbed size
- Mobility
- Repeatability
 - Control mobility
 - Control ambient influence (interfering foreign base stations, microwave ovens, ...)

Sustainability of test-beds





Thank you!

