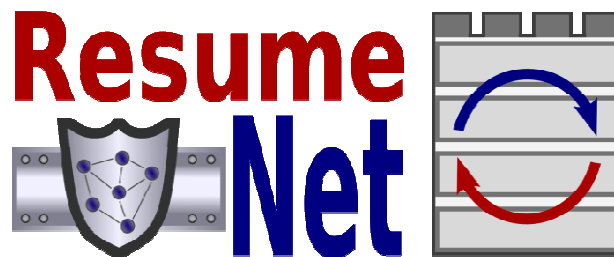




## Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation



Deliverable number:	D5.2c
Deliverable name:	Final Report on Dissemination and Standardization Activities
WP number:	5
Delivery date:	31.12.2011
Date of preparation:	31.12.2011
Editor:	C. Lac (FT)
Contributors:	C. Doerr (TUD), C. Lac (FT), C. Rohner (UU), M. Schoeller (NEC), P. Smith (ULanc)
Internal reviewers:	M. Karaliopoulos (U. of Athens)

## Summary

This deliverable reports on the different dissemination and standardization activities carried out during the third year of the ResumeNet project, and provides in its annex a synthesis of the publications during the first and second year of the project. These activities include:

- the maintenance of a public Web site (for external use) and Wiki pages (for daily internal use);
- the submission of research papers for publication in scientific journals and conferences/workshops of the field;
- the project presentations in symposia organized by, e.g., the European Commission;
- the use of additional communication channels (e.g., enterprise's Intranet) to publicize the concepts and objectives of the project;
- the organization, in collaboration with the Euro-NF NoE, of a network resilience PhD course on September 26-28, 2011 at ETH Zürich (Switzerland);
- the proposal and the management of a workshop on network resilience in the framework of the 30<sup>th</sup> IEEE Symposium on Reliable Distributed Systems 2011 (SRDS), on October 4, 2011 at the Escuela Técnica Superior de Ingenieros de Minas of the Universidad Politécnica de Madrid (Spain);
- the starting and the continuation of collaboration with institutions carrying out resilience-related activities in Europe, US, and Pacific region;
- the contribution of ResumeNet to standardization actions, i.e., 3GPP's SA2 group.

For each activity, the involved project consortium partners are explicitly mentioned.

## Table of contents

1. Web site and Wiki.....	1
2. Publications.....	1
2.1. Journals .....	1
2.2. Conferences and workshops.....	6
2.3. Ongoing work.....	14
3. Presentations .....	14
4. Publicity .....	15
5. ResumeNet summer school .....	15
6. Workshop on network resilience .....	17
7. Further impact.....	19
8. Contribution to standardization work.....	20
References.....	21
Annex .....	22

## 1. Web site and Wiki

Since the World Wide Web is a major dissemination channel, our first efforts in the project have been devoted to the creation of a Web site ([www.resumenet.eu](http://www.resumenet.eu)) in October 2008.

The Web site is structured along six components:

1. Project: it describes ResumeNet's main directions (framework, mechanisms, experimentation), the technical work packages, followed by a reminder of the project six-step strategy ( $D^2R^2+DR$ ), and a link to downloadable material summarizing the project scope and objectives.
2. Consortium: the partner institutions making up the consortium are quoted, together with a short description of each of them.
3. People and Roles: this zone shows the names and a short biography of i) members of the Advisory Board; ii) members of the different committees acting among the project; iii) researchers contributing to ResumeNet.
4. Results: the outcomes produced by ResumeNet's consortium are listed in this section through five categories, i.e., *Deliverables*, *Presentations* of the project objectives/results (in workshops, conferences, or meetings), *Publicity* (e.g., in newspaper articles), *Scientific papers* (in magazines, journals, conferences and workshops), *Standards* (results obtained in the framework of standardization groups).
5. News and Events: the past events where the project's members have taken dissemination actions, as well as upcoming ones, are summarized in this area.
6. Related Activities and Projects: this last section describes briefly national activities, EU projects (FP6, FP7, CELTICS) and other international projects in US and Pacific Region, whose scope lies close to the ResumeNet area of interests.

The project Web site has been updated continuously during year 3: this maintenance action has focused principally on the *Results* and *News & Events* sections.

The Wiki pages for the Consortium's daily work, effective since October 2008, constitute the private area used by all ResumeNet members to organize administrative, logistical, and technical tasks. In addition to this Wiki, an SVN server, hosted in ETHZ, is used for the collaborative production of all kinds of dissemination material including deliverables, reports, and publications.

## 2. Publications

As quoted in the DoW, "*Academic publications play an essential role to provide confidence to the outcomes of the project. Furthermore, it can be a starting point in the research area for further interest and discussion about the project topics and will lead to a higher degree of acceptance of new technologies. The transparency, given by academic publications, may be the enabler to trigger further interest of industries, provider and users to get acceptance for implementation of the project ideas in new products and services to establish resilience in the future Internet*" [DoW].

Research work carried out during this reporting period (September 2010 – December 2011) has been submitted, and, in most cases, accepted and published, to scientific journals, or conferences/workshops. The full set of publications/submissions covering the third year of the project is listed below, followed by a short description of their contents.

### 2.1. Journals

- A. Fischer, J.F. Botero, M. Duelli, D. Schlosser, X. Hesselbach, and H. De Meer, "ALEVIN - A framework to develop, compare, and analyze virtual network embedding algorithms", *Electronic Communications of the*

EASST (Proc. of the Workshop on Challenges and Solutions for Network Virtualization (NV), Kiel, Germany, March 10 2011), Vol. 37, 2011, pp. 1-12

Network virtualization is recognized as an enabling technology for the Future Internet. Applying virtualization of network resources leads to the problem of mapping virtual resources to physical resources, known as "Virtual Network Embedding" (VNE). Several algorithms attempting to solve this problem have been discussed in the literature, so far. However, comparison of VNE algorithms is hard, as each algorithm focuses on different criteria. To that end, we introduce a framework to compare different algorithms according to a set of metrics, which allow to evaluate the algorithms and compute their results on a given scenario for arbitrary parameters.

- W. Deng, M. Karaliopoulos, W. Mühlbauer, P. Zhu, X. Lu, and B. Plattner, "k-fault tolerance of the Internet AS graph", *Computer Networks (Elsevier)*, Vol. 55, N° 10, July 2011, pp. 2492-2503

Internet disruptions such as the Northeast Blackout (2003) and the Taiwan earthquake (2006) highlight the fragility of today's Internet. Our goal in this paper is to investigate the robustness of inter-domain communication at the level of autonomous systems (ASes), taking into account both topological connectivity and compliance to routing policies. To this end, we introduce the concept of  $k$ -fault tolerance for Type-of-Relationship (ToR) graphs, which requires that any two nodes (ASes) remain reachable from each other even after removing arbitrary  $k$  nodes from the AS graph. Our main contribution is theoretical and concerns the complexity of the  $k$ -fault tolerance decision problem. Drawing on strong evidence about the hierarchical structure of the Internet AS graph, we derive sufficient and necessary conditions for determining whether the graph is  $k$ -fault tolerant or not in polynomial time. We then apply this theoretical result to study the network-wide resilience properties of AS-level topology instances, as inferred from large-scale experimental data sets. We find that even single-node failures can disconnect up to hundred of ASes and that approximately 1500 ASes do not avail any real redundancy for their global reachability despite having two or more upstream links. Augmenting AS-level graphs for 1-fault tolerance improves overall resilience to failures, but requires a considerable number of AS-level edges (>7000) to be added. Interestingly, such additional upstream links are mainly needed at stub networks rather than at transit ASes, pointing out the need for multi-homing at stub networks.

- P. Smith, D. Hutchison, J.P.G. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. Lac, and B. Plattner, "Network resilience: a systematic approach", *IEEE Communications Magazine*, Vol. 49, N° 7, 2011, pp. 88-97

The cost of failures within communication networks is significant and will only increase as their reach further extends into the way our society functions. Some aspects of network resilience, such as the application of fault-tolerant systems techniques to optical switching, have been studied and applied to great effect. However, networks — and the Internet in particular — are still vulnerable to malicious attacks, human mistakes such as misconfigurations, and a range of environmental challenges. We argue that this is, in part, due to a lack of a holistic view of the resilience problem, leading to inappropriate and difficult-to-manage solutions. In this article, we present a systematic approach to building resilient networked systems. We first study fundamental elements at the framework level such as metrics, policies, and information sensing mechanisms. Their understanding drives the design of a distributed multilevel architecture that lets the network defend itself against, detect, and dynamically respond to challenges. We then use a concrete case study to show how the framework and mechanisms we have developed can be applied to enhance resilience.

- P. Van Mieghem, D. Stevanovic, F.A. Kuipers, C. Li, R. van de Bovenkamp, D. Liu, and H. Wang, "Decreasing the spectral radius of a graph by link removals", *Physical Review E*, Vol. 84, N° 1, July 2011

The decrease of the spectral radius, an important characterizer of network dynamics, by removing links is investigated. The minimization of the spectral radius by removing  $m$  links is shown to be an NP-complete

problem, which suggests considering heuristic strategies. Several greedy strategies are compared, and several bounds on the decrease of the spectral radius are derived. The strategy that removes that link  $l = i \sim j$  with largest product  $(x_1)_i(x_1)_j$  of the components of the eigenvector  $x_1$  belonging to the largest adjacency eigenvalue is shown to be superior to other strategies in most cases. Furthermore, a scaling law where the decrease in spectral radius is inversely proportional to the number of nodes  $N$  in the graph is deduced. Another sublinear scaling law of the decrease in spectral radius versus the number  $m$  of removed links is conjectured.

- J.P.G. Sterbenz, E.K. Çetinkaya, M.A. Hameed, A. Jabbar, S. Qian, and J.P. Rohrer, "Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation - invited paper", *Telecommunication Systems Journal* (available online September 2011)

As the Internet becomes increasingly important to all aspects of society, the consequences of disruption become increasingly severe. Thus it is critical to increase the resilience and survivability of future networks. We define resilience as the ability of the network to provide desired service even when challenged by attacks, large-scale disasters, and other failures. This paper describes a comprehensive methodology to evaluate network resilience using a combination of topology generation, analytical, simulation, and experimental emulation techniques with the goal of improving the resilience and survivability of the Future Internet.

- P. Van Mieghem, N. Blenn and C. Doerr, "Lognormal distribution in the Digg online social network", *The European Physical Journal B*, Vol. 83, No. 2, September 2011, pp. 251-261

We analyse the number of votes, called the digg value, which measures the impact or popularity of submitted information in the Online Social Network Digg. Experiments over five years indicate that the digg value of a story on the first frontpage follows closely a lognormal distribution. While the law of proportionate effect explains lognormal behavior, the proportionality factor  $a$  in that law is assumed to have a constant mean, whereas experiments show that  $a$  decreases linearly with time. Our hypothesis, the probability that a user diggs (votes) on a story given that he observes a certain digg value  $m$  equals  $a \times m$ , can explain observations, provided that the population of users that can digg on that story is close to a Gaussian.

- E.K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J.P.G. Sterbenz, "Modelling communication network challenges for future Internet resilience, survivability, and disruption tolerance: a simulation-based approach", *Telecommunication Systems Journal* (available online October 2011)

Communication networks play a vital role in our daily lives and they have become a critical infrastructure. However, networks in general, and the Internet in particular face a number of challenges to normal operation, including attacks and large-scale disasters, as well as due to mobility and the characteristics of wireless communication channels. Understanding network challenges and their impact can help us to optimise existing networks and improve the design of future networks; therefore it is imperative to have a framework and methodology to study them. In this paper, we present a framework to evaluate network dependability and performability in the face of challenges. We use a simulation-based approach to analyse the effects of perturbations to normal operation of networks. We analyse Sprint logical and physical topologies, synthetically generated topologies, and present a wireless example to demonstrate a wide spectrum of challenges. This framework can simulate challenges on logical or physical topologies with realistic node coordinates using the ns-3 discrete event simulator. The framework models failures, which can be static or dynamic that can temporally and spatially evolve. We show that the impact of network challenges depends on the duration, the number of network elements in a challenge area, and the importance of the nodes in a challenge area. We also show the differences between modelling the logical router-level and physical topologies. Finally, we discuss mitigation strategies to alleviate the impact of challenges.

- S. Tang, N. Blenn, C. Doerr and P. Van Mieghem, "Digging in the Digg social news website", IEEE Transactions on Multimedia, Vol. 13, No. 5, October 2011, pp. 1163-1175

The rise of social media aggregating websites provides platforms where users can actively publish, evaluate, and disseminate content in a collaborative way. In this paper, we present a large-scale empirical study about "Digg.com", one of the biggest social media aggregating websites. Our analysis is based on crawls of 1.5 million users and 10 million published stories on Digg. We study the distinct network structure, the collaborative user characteristics, and the content dissemination process on Digg. We empirically illustrate that friendship relations are used effectively in disseminating half of the content, although there exists a high overlap between the interests of friends. A successful content dissemination process can also be performed by random users who are browsing and digging stories. Since 88% of the published content on Digg is defined as news, it is important for the content to obtain sufficient votes in a short period of time before becoming obsolete. Finally, we show that the synchronization of users' activities in time is the key to a successful content dissemination process. The dynamics between users' voting activities consequently decrease the efficiency of friendship relations during content dissemination. The results presented in this paper define basic observations and measurements to understand the underlying mechanism of disseminating content in current online social news aggregators. These findings are helpful to understand the influence of service interfaces and user behaviors on content dissemination.

- C. Li, H. Wang, W. de Haan, C. J. Stam, and P. Van Mieghem, "The correlation of metrics in complex networks with applications in functional brain networks", Journal of Statistical Mechanics: Theory and Experiment (JSTAT), November 2011

An increasing number of network metrics have been applied in network analysis. If metric relations were known better, we could more effectively characterize networks by a small set of metrics to discover the association between network properties/metrics and network functioning. In this paper, we investigate the linear correlation coefficients between widely studied network metrics in three network models (Barabasi–Albert graphs, Erdős–Rényi random graphs and Watts–Strogatz small-world graphs) as well as in functional brain networks of healthy subjects. The metric correlations, which we have observed and theoretically explained, motivate us to propose a small representative set of metrics by including only one metric from each subset of mutually strongly dependent metrics. The following contributions are considered important. (a) A network with a given degree distribution can indeed be characterized by a small representative set of metrics. (b) Unweighted networks, which are obtained from weighted functional brain networks with a fixed threshold, and Erdős–Rényi random graphs follow a similar degree distribution. Moreover, their metric correlations and the resultant representative metrics are similar as well. This verifies the influence of degree distribution on metric correlations. (c) Most metric correlations can be explained analytically. (d) Interestingly, the most studied metrics so far, the average shortest path length and the clustering coefficient, are strongly correlated and, thus, redundant. Whereas spectral metrics, though only studied recently in the context of complex networks, seem to be essential in network characterizations. This representative set of metrics tends to both sufficiently and effectively characterize networks with a given degree distribution. In the study of a specific network, however, we have to at least consider the representative set so that important network properties will not be neglected.

- P. Van Mieghem, "The N-intertwined SIS epidemic network model", Computing (2011) 93, pp. 147-169

Serious epidemics, both in cyber space as well as in our real world, are expected to occur with high probability, which justifies investigations in virus spread models in (contact) networks. The N-intertwined virus spread model of the SIS-type is introduced as a promising and analytically tractable model of which the steady-state behavior is fairly completely determined. Compared to the exact SIS Markov model, the N-intertwined model makes only one approximation of a mean-field kind that results in upper bounding the exact model for finite network size N and improves in accuracy with N. We review many properties theoretically, thereby showing, besides the flexibility to extend the model into an entire heterogeneous setting, that much insight can be gained that is hidden in the exact Markov model.

- H. Wang, E. van Boven, A. Krishnakumar, M. Hosseini, H. van Hooff, T. Takema, N. Baken and P. Van Mieghem, "Multi-weighted monetary transaction network", *Advances in Complex Systems*, Vol. 14, No. 5, 2011, pp. 691-710

This paper aims to both develop and apply advances from the field of complex networks to large economic systems and explore the (dis)similarities between economic systems and other real-world complex networks. For the first time, the nature and evolution of the Dutch economy are captured by means of a data set analysis that describes the monetary transactions among 105 economical activity clusters over the period 1987–2007. We propose to represent this data set as a multi-weighted network, called the monetary transaction network. Each node represents a unique activity cluster. Nodes are interconnected via monetary transactions. The millions of euros that traverse the links and that circulate inside each activity cluster are denoted by a link weight and a node weight respectively. By applying innovative methodologies from network theory, we observe important features of the monetary transaction network as well as its evolution: (a) Activity clusters with a large internal flow tend to cooperate with many other clusters via high volume monetary transactions. (b) Activity clusters with a lower internal transaction volume prefer to transact with fewer neighboring nodes that have a higher internal flow. (c) The node weights seem to follow a power law distribution. Surprisingly, (b) and (c) have been observed in community structures of many real-world networks as well. (d) Activity clusters tend to balance the monetary volume of their transactions with their neighbors, reflected by a positive link weight correlation around each node. This correlation becomes stronger over time while the number of links increases over time as well.

- H. Wang, W. Winterbach and P. Van Mieghem, "Assortativity of complementary graphs", *The European Physical Journal B*, Vol. 83, No. 2, 2011, pp. 203-214

Newman's measure for (dis)assortativity, the linear degree correlation  $\rho_D$ , is widely studied although analytic insight into the assortativity of an arbitrary network remains far from well understood. In this paper, we derive the general relation (2), (3) and Theorem 1 between the assortativity  $\rho_D(G)$  of a graph  $G$  and the assortativity  $\rho_D(G_c)$  of its complement  $G_c$ . Both  $\rho_D(G)$  and  $\rho_D(G_c)$  are linearly related by the degree distribution in  $G$ . When the graph  $G(N, p)$  possesses a binomial degree distribution as in the Erdős-Rényi random graphs  $G_p(N)$ , its complementary graph  $G_c p(N) = G_{1-p}(N)$  follows a binomial degree distribution as in the Erdős-Rényi random graphs  $G_{1-p}(N)$ . We prove that the maximum and minimum assortativity of a class of graphs with a binomial distribution are asymptotically antisymmetric:  $\rho_{\max}(N, p) = -\rho_{\min}(N, p)$  for  $N \rightarrow \infty$ . The general relation (3) nicely leads to (a) the relation (10) and (16) between the assortativity range  $\rho_{\max}(G) - \rho_{\min}(G)$  of a graph with a given degree distribution and the range  $\rho_{\max}(G_c) - \rho_{\min}(G_c)$  of its complementary graph and (b) new bounds (6) and (15) of the assortativity. These results together with our numerical experiments in over 30 real-world complex networks illustrate that the assortativity range  $\rho_{\max} - \rho_{\min}$  is generally large in sparse networks, which underlines the importance of assortativity as a network characterizer.

- R. Holzer, and H. De Meer, "Methods for approximations of quantitative measures in self-organizing systems", in "Self-organizing systems" (C. Bettstetter, and C. Gershenson, Eds.), *Lecture Notes in Computer Science*, Vol. 6557, 2011, Springer-Verlag, pp. 1-15

For analyzing properties of complex systems, a mathematical model for these systems is useful. In micro-level modeling, a multigraph can be used to describe the connections between objects. The behavior of the objects in the system can be described by (stochastic) automata. In such a model, quantitative measures can be defined for the analysis of the systems or for the design of new systems. Due to the high complexity, it is usually impossible to calculate the exact values of the measures, so approximation methods are needed. In this paper we investigate some approximation methods to be able to calculate quantitative measures in a micro-level model of a complex system. To analyze the practical usability of the concepts, the methods are applied to a slot synchronization algorithm in wireless sensor networks.



- W. Winterbach, H. Wang, M. Reinders, P. Van Mieghem and D. de Ridder, "Metabolic network destruction: relating topology to robustness", *Nano Communication Networks*, Vol. 41, No. 6, 2011, pp. 365-72

Biological networks exhibit intriguing topological properties such as small-worldness. In this paper, we investigate whether the topology of a particular type of biological network, a metabolic network, is related to its robustness. We do so by perturbing a metabolic system in silico, one reaction at a time and studying the correlations between growth, as predicted by flux balance analysis, and a number of topological metrics, as computed from three network representations of the metabolic system. We find that a small number of metrics correlate with growth and that only one of the network representations stands out in terms of correlated metrics. The most correlated metrics point to the importance of hub nodes in this network, so-called "currency metabolites". Since they are responsible for interconnecting distant functional modules in the network, they are important points in the network for predicting if reaction removal affects growth. A second set of correlations in contrast is related to "loner" nodes that uniquely connect important pathways and thus correspond to essential steps in metabolism.

- X. Ge and H. Wang, "Community overlays upon real-world complex networks", to appear in *The European Physical Journal B*

Many networks are characterized by the presence of communities, densely intra-connected groups with sparser inter-connections between groups. We propose a community overlay network representation to capture large-scale properties of communities. A community overlay  $G_0$  can be constructed upon a network  $G$ , called the underlying network, by (a) aggregating each community in  $G$  as a node in the overlay  $G_0$ , (b) connecting two nodes in the overlay if the corresponding two communities in the underlying network have a number of direct links in between, (c) assigning to each node/link in the overlay a node/link weight, which represents, e.g., the percentage of links in/between the corresponding underlying communities. The community overlays have been constructed upon a large number of real-world networks based on communities detected via five algorithms. Surprisingly, we find the following seemingly universal properties: (i) an overlay has a smaller degree-degree correlation than its underlying network  $\rho_0(D_{i+}, D_{i-}) < \rho(D_{i+}, D_{i-})$  and is mostly disassortative  $\rho_0(D_{i+}, D_{i-}) < 0$ ; (ii) a community containing a large number  $W_i$  of nodes tends to connect to many other communities  $\rho_0(W_i, D_i) > 0$ . We explain the generic observation (i) by two facts: (1) degree-degree correlation or assortativity tends to be positively correlated with modularity; (2) by aggregating each community as a node, the modularity in the overlay is reduced and so is the assortativity. The observation (i) implies that the assortativity of a network depends on the aggregation level of the network representation, which is illustrated by the Internet topology at router and AS level.

## 2.2. Conferences and workshops

- J. Omic, J. Martin-Hernandez, and P. Van Mieghem, "Network protection against worms and cascading failures using modularity partitioning", *International Teletraffic Congress (ITC 22)*, Amsterdam, The Netherlands, September 7-9, 2010

Communication networks are prone to virus and worms spreading and cascading failures. Recently, a number of social networking worms have spread over public Web sites. Another example is error propagation in routing tables, such as in BGP tables. The immunization and error curing applied to these scenarios are not fast enough. There have been studies on the effect of isolating and curing network elements, however, the proposed strategies are limited to node removals. This paper proposes a link isolation strategy based on the quarantining of susceptible clusters in the network. This strategy aims to maximize the epidemic control while minimizing the impact on the clusters performance. We empirically study the influence of clustering on robustness against epidemics in several real-world and artificial networks. Our results show an average curing rate improvement above 50% for the studied real-world networks under analysis.

- C. Lac, N. Kheir, and B. Delosme, "Securing a communicating object data platform", LambdaMu 17, La Rochelle, France, October 5-7, 2010 (in French)

The widespread use of smart mobile devices, together with identifiers (bar codes, RFID, ...) embedded in the objects/products, enables communication with, and about, these objects/products. This usage (r)evolution, opening the way for the Internet of Things, induces major changes in the retail business. The ICOM project (Infrastructure for the Future Trade) is developing a mutualized technical platform allowing exchanges between applications across heterogeneous hardware and software. This intra(inter)-enterprise infrastructure connects objects, identified in various ways, with the enterprise(s) information systems and fixed/mobile terminals and/or, to a lesser extent, between them. Several modules comprise this middleware: data acquisition and formatting; filtering, routing and transport based on these data contents; traceability/persistence; distributed objects name server. A platform, based on a messages publication/broadcast through subscription model (PubSub), realizes the filtering and routing functions. This paper presents an approach for securing a PubSub platform: availability and security (confidentiality, data integrity) are the targeted resilience criteria. After a risk analysis, we define the nominal security policy, and the threat contexts, in terms of dependability and security. The actions to launch will be detailed following the mapping linking the threat contexts to the response rules. Disabling these contexts and deploying the reaction policies form the final stage of the approach. Applying this securing process to the ICOM's PubSub platform will then be detailed. The tasks remaining to be done in order to complete the study conclude the article.

- E.K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J.P.G. Sterbenz, "A comprehensive framework to simulate network attacks and challenges", 2nd IEEE International Workshop on Reliable Networks Design and Modelling (RNDM), Moscow, Russia, October 18-20, 2010

Communication networks have evolved tremendously over the past several decades, offering a multitude of services while becoming an essential critical infrastructure in our daily lives. Networks in general, and the Internet in particular face a number of challenges to normal operation, including attacks and large-scale disasters, as well as due to the characteristics of the mobile wireless communication environment. It is therefore vital to have a framework and methodology for understanding the impact of challenges to harden current networks and improve the design of future networks. In this paper, we present a framework to evaluate network dependability and performability in the face of challenges. This framework uses ns-3 simulation as the methodology for analysis of the effects of perturbations to normal operation of the networks, with a challenge specification applied to the network topology. This framework can simulate both static and dynamic challenges based on the failure or wireless-impairment of individual components, as well as modelling geographically-correlated failures. We demonstrate this framework with the Sprint Rocketfuel and synthetically generated topologies as well as a wireless example, to show that this framework can provide valuable insight for the analysis and design of resilient networks.

- L. Braun, A. Didebulidze, N. Kammenhuber, and G. Carle, "Comparing and improving current packet capturing solutions based on commodity hardware", Internet Measurement Conference (IMC), Melbourne, Australia, November 1-3, 2010

Capturing network traffic with commodity hardware has become a feasible task: advances in hardware as well as software have boosted off-the-shelf hardware to performance levels that some years ago were the domain of expensive special purpose hardware. However, the capturing hardware still needs to be driven by a well-performing software stack in order to minimize or avoid packet loss. Improving the capturing stack of Linux and FreeBSD has been an extensively covered research topic in the past years. Although the majority of the proposed enhancements have been backed by evaluations, these have mostly been conducted on different hardware platforms and software versions, which renders a comparative assessment of the various approaches difficult, if not impossible. This paper summarizes and evaluates the performance of current packet capturing solutions based on commodity hardware. We identify bottlenecks and pitfalls within the capturing stack of FreeBSD and Linux, and give explanations for the observed effects. Based on our experiments, we provide guidelines for users on how to configure their capturing systems for

optimal performance and we also give hints on debugging bad performance. Furthermore, we propose improvements to the operating system's capturing processes that reduce packet loss, and evaluate their impact on capturing performance.

- T. Taleb, Y. Hadjadj-Aoul, and A. Benslimane, "Integrating security with QoS in Next Generation Networks", IEEE Globecom, Miami, FL, USA, December 6-12, 2010

Along with recent Internet security threats, different security measures have emerged. Whilst these security schemes ensure a level of protection against security threats, they often have significant impact on the perceived Quality of Service (QoS). There is thus need to retrieve ways for an efficient integration of security requirements with their QoS counterparts. In this paper, we devise a Quality of Protection framework that tunes between security requirements and QoS using a multi-attribute decision making model. The performance of the proposed approach is evaluated and verified via a use-case study using computer simulations.

- M.A. Hameed, A. Jabbar, E.K. Çetinkaya, and J.P.G. Sterbenz, "Deriving network topologies from real world constraints", IEEE GLOBECOM Workshop on Complex and Communication Networks (CCNet), Miami, FL, USA, December 12 2010, pp. 415–419

Realistic network topologies are crucial for network research and are commonly used for the analysis, simulation, and evaluation of various mechanisms and protocols. In this paper, we discuss network topology models to generate physical topologies for backbone networks. In order to gain better understanding of current topologies and engineer networks for the future, it is necessary to generate realistic physical topologies that are governed by the infrastructure as opposed to only logical topologies that are governed by policy or higher-layer abstractions. The objective of this work is to present the principles that are key to node distributions of realistic topologies and the challenges involved. We argue that the dominant factors that influence the location of the PoPs are population density distribution and the technology penetration of a given region. Hence we implement a clustering algorithm to accurately predict the location of PoPs and later explore cost constrained models to generate realistic physical topologies.

- J.P.G. Sterbenz, E.K. Çetinkaya, M. Hameed, A. Jabbar, and J.P. Rohrer, "Modelling and analysis of network resilience", 3rd International Conference on Communication Systems and Networks (COMSNETS), Bangalore, India, January 4-8, 2011 (invited paper)

As the Internet becomes increasingly important to all aspects of society, the consequences of disruption become increasingly severe. Thus it is critical to increase the resilience and survivability of the future network. We define resilience as the ability of the network to provide desired service even when challenged by attacks, large-scale disasters, and other failures. This paper describes a comprehensive methodology to evaluate network resilience using a combination of analytical and simulation techniques with the goal of improving the resilience and survivability of the Future Internet.

- A. Schaeffer-Filho, P. Smith, and A. Mauthe, "Policy-driven network simulation: a resilience case study", 26th ACM Symposium on Applied Computing (SAC), Taichung, Taiwan, March 21-24, 2011

Networks must be resilient to challenges such as malicious attacks or network overload and adapt their operation in an autonomous manner. Network simulations enable the testing of complex network scenarios (which would be difficult to emulate using actual hardware) in an inexpensive manner. However, it is difficult to evaluate resilience strategies that involve the interplay between a number of detection and remediation mechanisms that must be activated on demand according to events observed in the network (as opposed to hardcoded protocols). In this paper we propose the notion of a policy-based resilience simulator based on the integration of a network simulator and a policy management framework. This permits the evaluation of resilience strategies consisting of mechanisms whose behaviour can be adapted during runtime - e.g. setting flags, dropping connections, triggering or stopping monitoring sessions, etc. We employ policies to specify the required adaptations, which are de-coupled from the hard-wired

implementations of the simulated components, according to conditions observed during run-time in the simulation. We can thus observe how real policies affect the operation and the behaviour of simulated components, and then evaluate the effectiveness of resilience strategies before they are deployed in the network infrastructure.

- C. Doerr, "Parallelized network-driven analysis of network systems on commodity hardware", IEEE International Conference on Networking, Sensing and Control, Delft, Netherlands, April 11-13, 2011

In recent times, the study of complex network systems, for example communication networks such as the Internet, Smart Grids or Social Networks, have received significant attention. While newly emerging data sets in these domains now allow for a broad quantitative exploration and empirical validation of theoretical models towards a better understanding of complex networks, the enormous size of complex networks make many analyses too computationally expensive, therefore rendering an effective study in most cases impractical. This paper argues that through parallelization and network-driven analysis an effective study becomes again feasible, and that such parallelization may even be achieved using commodity hardware, thus making this technique applicable to a broad community.

- J.P. Rohrer, E.K. Çetinkaya, and J.P.G. Sterbenz,, "Progress and challenges in large-scale future Internet experimentation using the GpENI programmable testbed", 6th ACM International Conference on Future Internet Technologies (CFI), Seoul, Korea, June 13-15, 2011

GpENI is evolving to provide a promising environment in which to do experimental research in the resilience and survivability of future networks, by allowing programmable control over topology and mechanism, while providing the scale and global reach needed to conduct network experiments far beyond the capabilities of a conventional testbed. Addressing this need at scale introduces a number of challenges both in deployment and in collecting results that can be directly compared to simulation results for cross-verification purposes. In this short paper, we present the scope, design goals, challenges, and current status of the GPENI programmable testbed, as well as an overview and examples of the types of experiments we are beginning to run.

- M. Duelli, D. Schlosser, J.F. Botero, X. Hesselbach, A. Fischer and H. De Meer , "VNREAL: Virtual Network Resource Embedding ALgorithms in the Framework ALEVIN", 7th Euro-NF Conference on Next Generation Internet, Kaiserslautern, Germany, June 27-29, 2011, pp. 1-2

Network virtualization is recognized as an enabling technology for the Future Internet that overcomes network ossification. However, it introduces a set of challenges. In any network virtualization environment, the problem of optimally mapping virtual resources to physical resources, known as virtual network embedding (VNE), is a critical challenge. Several algorithms attempting to solve this problem have been proposed in literature, so far. However, comparison of existing and new VNE algorithms is hard, as each algorithm focuses on different criteria. To that end, the VNREAL project introduces ALEVIN, a framework to compare different algorithms according to a set of metrics, easily incorporate new VNE algorithms, and evaluate these algorithms on a given scenario for arbitrary parameters.

- J.F. Botero, X. Hesselbach, M. Duelli, D. Schlosser, A. Fischer and H. De Meer , "Flexible VNE algorithms analysis using ALEVIN", 11th Würzburg Workshop on IP: Joint ITG and Euro-NF Workshop "Visions of Future Generation Networks" (EuroView 2011), Würzburg, Germany, August 1-2, 2011

Network virtualization is recognized as an enabling technology for the Future Internet that overcomes network ossification. However, it introduces a set of challenges. In any network virtualization environment, the problem of optimally mapping virtual demands to physical resources, known as virtual network embedding (VNE), is a crucial challenge. This paper analyses the behaviour of the main algorithms proposed to solve VNE by means of the ALEVIN framework. The VNE algorithms are evaluated with regard to appropriate metrics such as: cost, revenue, and virtual network acceptance ratio. We also analyze the impact of the recently introduced hidden hop demand concept in the performance of the VNE algorithms.

- J.P. Rohrer, E.K. Çetinkaya, and J.P.G. Sterbenz, "Resilience experiments in the GpENI programmable future Internet testbed", 11th Würzburg Workshop on IP: Joint ITG and Euro-NF Workshop "Visions of Future Generation Networks" (EuroView 2011), Würzburg, Germany, August 1-2, 2011

Testbeds play an important role in evaluating new protocols, and GpENI (Great Plains Environment for Network Innovation) is a Future Internet research testbed that provides worldwide scalability to researchers to conduct their experiments. We describe experiments for which GpENI will be used, with emphasis on network infrastructure resilience. GpENI is part of the GENI and FIRE programs.

- F. Bjurefors, P. Gunningberg, C. Rohner, and S. Tavakoli, "Congestion avoidance in a data-centric opportunistic network", ACM SIGCOMM Workshop on Information-Centric Networking (ICN 2011), Toronto, ON, Canada, August 19, 2011

In order to achieve data delivery in an opportunistic network, data is replicated when it is transmitted to nodes within communication reach and that are likely to be able to forward it closer to the destination. This replication and the unpredictable contact times due to mobility necessitate buffer management strategies to avoid buffer overflow on nodes. In this paper, we investigate buffer management strategies based on local forwarding statistics and relevance of the data for other nodes. The results obtained on our emulation platform for opportunistic networks show that strategies with a high data refresh rate achieve the most efficient delivery and generate the smallest overhead on our community and mobility scenarios.

- A.A. Beshir, F.A. Kuipers, A. Orda, and P. Van Mieghem, "Survivable impairment-aware traffic grooming in WDM rings", 23rd International Teletraffic Congress, San Francisco, CA, USA, September 6-8, 2011

Wavelength Division Multiplexing (WDM) optical networks offer a large amount of bandwidth using multiple, but independent wavelength channels (or lightpaths), each operating at several Gb/s. Since the traffic between users is usually only a fraction of the capacity offered by a wavelength, several independent traffic streams can be *groomed* together. In addition, in order to reverse the effect of noise and signal degradations (physical impairments), optical signals need to be regenerated after a certain *impairment threshold* is reached. We consider *survivable* impairment-aware traffic grooming in WDM rings, which are among the most widely deployed optical network topologies. We first show that the survivable impairment-aware traffic grooming problem, where the objective is to minimize the total cost of grooming and regeneration, is NP-hard. We then provide approximation algorithms (for uniform traffic), and efficient heuristic algorithms whose performance is shown to be close to the lower-bounds (for non-uniform traffic) both when (1) the impairment threshold can be ignored, and (2) the impairment threshold should be considered.

- A. Fischer, A. Fessi, G. Carle, and H. de Meer, "Wide-area virtual machine migration as resilience mechanism", International Workshop on Network Resilience (WNR), Madrid, Spain, October 4, 2011

The resilience of services in the Internet has become an important issue and is expected to become even more important in the future. Virtualization is one of the means which can be deployed for resilience purposes. In this paper we follow a systematic approach to the use of virtualization to increase the resilience of network services. First, we provide an analysis of the potential failures of services running within Virtual Machines (VM) and how VM migration or replication can be used to address these failures. Then, we address the problem of re-establishing connectivity between a service and its clients upon successful migration, by leveraging results from mobility research. A special focus is given to wide-area VM migration, since it is considered as the solution for some difficult failures, e.g., large-scale failures due to natural disasters.

- J.P. Rohrer and J.P.G. Sterbenz, "Predicting topology survivability using path diversity", 3rd International Workshop on Reliable Networks Design and Modeling (RNDM), Budapest, Hungary, October 5-7 2011

In this paper we extend our path diversity metric to create a composite compensated total graph diversity metric that is representative of a particular topology's survivability with respect to distributed simultaneous link and node failures. We tune the accuracy of this metric using 17 topologies, including 3 real fiber maps, 10 inferred logical maps, and 2 synthetic topologies having simulated their performance under a range of failure severities, and present the results. The topologies used are from national-scale backbone networks, with a variety of characteristics, which we characterize using standard graph theoretic metrics. The end result is a compensated total graph diversity metric that accurately predicts the survivability of a given network topology.

- M. Schöller, P. Smith, and D. Hutchison, "Assessing risk for network resilience", 3rd International Workshop on Reliable Networks Design and Modeling (RNDM), Budapest, Hungary, October 5-7 2011

Communication networks and the Internet, in particular, have become a critical infrastructure for daily life, business and governance. Various challenging conditions can render networks or parts thereof unusable, with severe consequences. Protecting a network from all possible challenges is infeasible because of monetary, hardware and software constraints. Hence, a methodology to measure the risk imposed by the various challenges threatening the system is a necessity. In this paper, we present a risk assessment process to identify the challenges with the highest potential impact to a network and its users. The result of this process is a prioritised list of challenges and associated system faults, which can guide network engineers towards the mechanisms that have to be built into the network to ensure network resilience, whilst meeting cost constraints. Furthermore, we discuss how outcomes from the intermediate steps of our risk assessment process can be used to inform network resilience design. A better understanding of these aspects and a way to determine reliable measures are open issues, and represent important new research items in the context of resilient and survivable networks.

- E. Gourdin, J. Omic, and P. Van Mieghem, "Optimization of network protection against virus spread", 8th Int. Workshop Design of Reliable Communication Networks (DRCN), Krakow, Poland, October 10-12, 2011

The effect of virus spreading in a telecommunication network, where a certain curing strategy is deployed, can be captured by epidemic models. In the N-intertwined model proposed, the probability of each node to be infected depends on the curing and infection rate of its neighbors. In this paper, we consider the case where all infection rates are equal and different values of curing rates can be deployed within a given budget, in order to minimize the overall infection of the network. We investigate this difficult optimization together with a related problem where the curing budget must be minimized within a given level of network infection. Some properties of these problems are derived and several solution algorithms are proposed. These algorithms are compared on two real world network instances, while Erdős-Rényi graphs and some special graphs such as the cycle, the star, the wheel and the complete bipartite graph are also addressed.

- A. Jabbar, H. Narra, and J.P.G. Sterbenz,, "An approach to quantifying resilience in mobile ad hoc networks", 8th Int. Workshop Design of Reliable Communication Networks (DRCN), Krakow, Poland, October 10-12, 2011

Resilience is the ability of a network to provide acceptable service in the presence of challenges to normal operations. With increasing significance of resilience in modern communications infrastructure and services, there is a need for rigorous quantitative evaluation of resilience. In this paper, we present a framework to quantify resilience between any two layers in the network stack. Resilience is quantified as a function of state transitions wherein states are defined as aggregation of points in the two orthogonal dimensions of operational and service state. This approach is applied to the case of mobile ad hoc networks in order to determine the resilience of various levels to the perturbations in the normal operations of the network. Simulation results show that this framework provides a tractable approach and abstraction to quantify multilevel resilience.

- Y. Yu, M. Fry, A. Schaeffer-Filho, P. Smith, and D. Hutchison, "An adaptive approach to network resilience: evolving challenge detection and mitigation", 8th Int. Workshop Design of Reliable Communication Networks (DRCN), Krakow, Poland, October 10-12, 2011

It is widely agreed that computer networks need to become more resilient to a range of challenges that can seriously impact their normal operation. Challenges include malicious attacks, misconfigurations, accidental faults and operational overloads. As part of an overall strategy for network resilience, a crucial requirement is the identification of challenges in real-time, followed by the application of appropriate remedial action. In this paper, we motivate and describe a novel solution that enables the progressive multi-stage deployment of resilience strategies, based on incomplete challenge and context information. Policies are used to orchestrate the interactions between various resilience mechanisms, which incrementally identify the nature of a challenge and deploy appropriate remediation mechanisms. We demonstrate the benefits of this approach via simulation of a resource starvation attack on an Internet Service Provider infrastructure. By initially using lightweight detection and then progressively applying more heavyweight analysis, a key contribution of our work is the ability to mitigate a challenge as early as possible and rapidly detect its root cause. The approach we propose in this paper has the flexibility, reproducibility and extensibility needed to assist in the identification and remediation of various network challenges in the future.

- R. Holz, L. Braun, N. Kammenhuber, and G. Carle, "The SSL landscape - a thorough analysis of the X.509 PKI using active and passive measurements", 11th Annual Internet Measurement Conference (IMC), Berlin, Germany, November 2-4, 2011

The SSL and TLS infrastructure used in important protocols like HTTPs and IMAPs is built on an X.509 public key infrastructure (PKI). X.509 certificates are thus used to authenticate services like online banking, shopping, e-mail, etc. However, it always has been felt that the certification processes of this PKI may not be conducted with enough rigor, resulting in a deployment where many certificates do not meet the requirements of a secure PKI. This paper presents a comprehensive analysis of X.509 certificates in the wild. To shed more light on the state of the deployed and actually used X.509 PKI, we obtained and evaluated data from many different sources. We conducted HTTPs scans of a large number of popular HTTPs servers over a 1.5-year time span, including scans from nine locations distributed over the globe. To compare certification properties of highly ranked hosts with the global picture, we included a third-party scan of the entire IPv4 space in our analyses. Furthermore, we monitored live SSL/TLS traffic on a 10Gbps uplink of a large research network. This allows us to compare the properties of the deployed PKI with the part of the PKI that is being actively accessed by users. Our analyses reveal that the quality of certification lacks in stringency, due to a number of reasons among which invalid certification chains and certificate subjects give the most cause for concern. Similar concerns can be raised for other properties of certification chains and also for many self-signed certificates used in the deployed X.509 PKI. Our findings confirm what has long been believed – namely that the X.509 PKI that we use so often in our everyday's lives is in a sorry state.

- M. Nassar, S. Martin, G. Leduc, and O. Festor, "Using decision trees for generating adaptive SPIT signatures", 4th Int. Conference on Security of Information and Networks (SIN), Sydney, Australia, November 14-19, 2011

With the spread of new and innovative Internet services such as IP communications, the challenge of protecting and defending these critical applications has been raised. In particular, the Application Layer Firewalls (ALFs) attempt to filter the unwanted activities based on the knowledge of the running applications. Optimizing the ALF configuration at a given time by selecting the best filtering rules is problematic because it depends on both natures of the legal traffic and the unwanted activities. More precisely, we do not know exactly how the unwanted activities are reflected in the messages of the application protocols. We argue that the solution of this problem can be adaptively learnt by using adaptive decision trees. In particular, we address the case of Spam over Internet Telephony (SPIT) mitigation in the context of the Session Initiation Protocol (SIP) and Voice over IP (VoIP) networks. Our simulations show

that quickly learning the optimal configuration for a SIP firewall leads to reduce at lowest the unsolicited calls reported by the users under protection. Our results promote the application of machine learning algorithms for supporting network and service resilience against such new challenges.

- T. Taleb, and K. Samdanis, "Ensuring service resilience in the EPS: MME failure restoration case", IEEE Globecom 2011, Houston, Texas, USA, December 5-9 2011

In the Evolved Packet System (EPS), service resiliency can be heavily impacted by a node failure, especially in its control plane. Ensuring service resiliency via defining efficient and proactive restoration mechanisms is of vital importance. In this paper, we address the case of Mobility Management Entity (MME) failure. We propose schemes for MME failure detection and restoration considering User Equipments (UEs) in both idle and active mode. As a MME failure may impact a potential number of UEs, network signaling overload control, via randomized paging and handling signaling messages in bulk, is considered. The proposed schemes are evaluated through simulations and encouraging results are obtained.

- M. Karaliopoulos, and C. Rohner, "Trace-based performance analysis of opportunistic forwarding under imperfect cooperation conditions", INFOCOM 2012 Mini-Conference, Orlando, FL, USA, March 25-30 2012

The paper proposes an innovative method for the performance analysis of opportunistic forwarding protocols over files logging mobile node encounters (contact traces). The method is modular and evolves in three main processing steps. It first carries out trace inflation to systematically identify those contacts that constitute message forwarding opportunities for given message coordinates and forwarding rules. It then draws on graph expansion techniques to capture these forwarding contacts into sparse space-time graph representations (constructs). Finally, it runs standard shortest path algorithms over these constructs and derives typical performance metrics such as message delivery delay and path hop count. The method is flexible in that it can easily assess the protocol operation under various expressions of imperfect node cooperation. We describe it in detail, analyze its complexity, and assess it against discrete event simulations for three representative randomized forwarding schemes. The match with the simulation results is excellent and obtained with run times up to three orders of size smaller than the duration of the simulations, thus rendering our method a valuable tool for the performance analysis of opportunistic forwarding schemes.

- S.M. Günther, J. Schlamp, and G. Carle, "Spring-based geolocation", to be presented in 13th IEEE/IFIP Network Operations and Management Symposium (NOMS), Maui, HI, USA, April 2012

Given an IP address, it is a challenging task to obtain its geographic location. Besides approaches which associate coordinates with IP addresses in a predominantly static way, there are also measurement based approaches that exploit the correlation between the propagation delay of signals and round trip times of probe packets. We analyze multiple approaches solely based on delay measurements, i.e., without the use of third-party knowledge, and obtain mean errors of just under 100 km. In this paper, we propose a new model for IP geolocation which combines the strengths of different previous techniques and reduces IP geolocation to the problem of finding equilibrium points in a spring system. Our approach, called Spring-Based Geolocation (SBG), is able to reduce the mean error to less than 75 km in our experiments without adding significant complexity. In fact, our model allows for additional data sources in a natural way, which has the potential to further improve results.

- A. Schaeffer-Filho, P. Smith, A. Mauthe, D. Hutchison, Y. Yu and M. Fry, "A framework for the design and evaluation of network resilience strategies", to be presented in 13th IEEE/IFIP Network Operations and Management Symposium (NOMS), Maui, HI, USA, April 2012

Network resilience strategies aim to maintain acceptable levels of network operation in the face of challenges, such as malicious attacks, operational overload or equipment failures. Often the nature of these challenges requires resilience strategies comprising mechanisms across multiple protocol layers and in disparate locations of the network. In this paper, we address the problem of resilience management and



advocate that a new approach is needed for the design and evaluation of resilience strategies. To support the realisation of this approach we propose a framework that enables (1) the offline evaluation of resilience strategies to combat several types of challenges, (2) the generalization of successful solutions into reusable patterns of mechanisms, and (3) the rapid deployment of appropriate patterns when challenges are observed at run-time. The evaluation platform permits the simulation of a range of challenge scenarios and the resilience strategies used to combat these challenges. Resilience strategies that can successfully address a particular type of challenge can be promoted to become resilience patterns. Patterns can thus be used to rapidly deploy resilience configurations of mechanisms when similar challenges are detected in the live network.

### 2.3. Ongoing work

In addition to the publications listed above, there are 8 papers under review/submission covering work done in the project.

- T. Jung, D. Ernst, S. Martin, M. Nassar, and G. Leduc, "Towards SPIT filters with optimal performance guarantees" – submitted to Telecommunication Systems (Springer)
- T. Taleb et al., "QoS2: a framework for integrating quality of security with quality of service" – submitted to Wiley Journal on Security and Communication Networks
- P. Van Mieghem, C. Doerr, H. Wang, J. Martin Hernandez, D. Hutchison, M. Karaliopoulos, and R. Kooij, "Towards a framework for computing topological network robustness" – submitted to Computer Communications (Elsevier)
- S. Martin, L. Chiarello, and G. Leduc, "DISco: a distributed information store for network challenges and their outcome" – submitted to DANMS, Maui, HI, USA, April 16-20, 2012
- S. Natouri, and C. Lac, "Towards a real-time service resilience framework" – submitted to LambdaMu18, Tours, France, October 16-18, 2012
- T. Jung, D. Ernst, S. Martin, and G. Leduc, "A framework for a self-learning security layer based on contextual multi-armed bandits" – under submission
- G. Popa, "Characterization of random linear network coding with application to broadcast optimization in intermittently connected networks" – under submission
- G. Popa, F. Legendre, M. Karaliopoulos, and E. Gourdin, "Avoiding interference improves collaboration in multi-hop networks" – under submission

### 3. Presentations

Contributing to, and participating in, dissemination events, e.g., organized by the European Commission, is part of ResumeNet commitments. To this end, seven presentations on various aspects of the project, e.g., virtualization mechanisms and resilience assessment, have been given in 2010/2011.

- M. Schöller, "Resilience and survivability in communication networks: strategies, principles, and survey of disciplines", Karlsruhe Institute for Technology, Germany, November 22, 2010
- A. Fischer, and H. de Meer, "Resilience in networks: elements and approach for a trustworthy infrastructure", Future Internet Assembly, Ghent, Belgium, December 16-17, 2010

- M. Schöller, "Network virtualization - An enabler for network resilience?", Karlsruhe Institute for Technology, Germany, February 09, 2011
- G. Carle, "Network resilience: from concepts to experimentation", FIRE Research Workshop at Future Internet Week, Budapest, Hungary, May 16, 2011
- P. Van Mieghem, "Virus spread in networks", Keynote Presentation, International Workshop on Modeling, Analysis, and Control of Complex Networks (Cnet), San Francisco, CA, USA, September 9, 2011
- P. Van Mieghem, "Robustness of complex networks", Tutorial, 8th International Workshop on Design of Reliable Communication Networks (DRCN), October 10, 2011, Krakow, Poland
- P. Smith, "The importance of resilience in the future Internet: framework, mechanisms and experiments", Future Internet Assembly, Poznan, Poland, October 25, 2011

Download link: [www.resumenet.eu/results/presentations](http://www.resumenet.eu/results/presentations)

## 4. Publicity

- C. Lac, E. Gourdin, and B. Delosme, "ResumeNet: networks and services resilience", Orange Group Innovation Division Intranet, November 2010 (in French)

Download link: [www.resumenet.eu/results/publicity](http://www.resumenet.eu/results/publicity)

## 5. ResumeNet summer school

In collaboration with the Euro-NF NoE [ENF], ResumeNet organized a network resilience PhD Course on September 26-28, 2011 at ETH Zürich (Switzerland). The three day event covered widespread network resilience aspects, including exercises. 16 students from six countries attended the course; their feedback was very positive and encouraging. As a result, ResumeNet will provide a set of slides which will help others to integrate network resilience into their courses.

The series of eight lectures and exercises, conducted by international teachers (see below), surveyed fundamental and applied aspects of network resilience, and identified novel opportunities and research directions in this area. The school also provided the participants a great opportunity to meet other students working in the field, to establish contacts that may lead to research collaborations in the future. The intended audience was graduate students, PhD students and young researchers from universities and industrial laboratories around Europe. The lectures were complemented with a highly appreciated guest lecture "Best current practices" by Simon Leinen from the Swiss academic network provider SWITCH.

The course was kindly sponsored by Euro-NF which provided funding for lunches and a reception at Hotel du Theatre allowing lively interaction between students and teachers. Euro-NF also supported the traveling for students from partners associated to Euro-NF. This effort was led by Dr. C. Rohner (U. of Uppsala) with help from some ResumeNet partners [RES]. The programme of this three day event was as follows.

- Resilience principles and related disciplines (Prof. J.P.G. Sterbenz, U. of Kansas)

This talk covered the basic principles of network resilience, including definitions of fundamental approaches to resilience, such as diversity and redundancy. Furthermore, the talk placed resilience with context of related disciplines, such as survivability and fault tolerance, for example. The aim was to give the student a foundation in resilience topics that were built on in the rest of the course.

- Resilience metrics (Prof. J.P.G. Sterbenz, U. of Kansas)

Appropriate metrics are fundamental to understanding the resilience of a given network deployment. They form an essential part of off-line decision processes, such as risk assessment and whether to invest in new infrastructure for resilience, and on-line processes that monitor the health of a network and the supported services. Initially, this talk has presented a survey of resilience metrics. It was then continued by investigating approaches to measuring and evaluating network resilience, which is a multi-level issue, i.e., the behaviour of metrics at different layers is often correlated.

- Modeling the network operation under challenges and assessing its resilience (Dr. M. Karaliopoulos, U. of Athens)

The talk attempted a survey of theoretical methods and tools that are used for the analytical assessment of networks' resilience. It first covered classical reliability and performability analysis techniques addressing hardware/software failures and network performance, iterated over fundamental tools such as Markovian models and Petri Nets that dominated this area, and outlined approaches to the assessment of resilience in more novel network paradigms such as the wireless mesh and delay tolerant networks.

- Resilient routing (Dr. C. Rohner, U. of Uppsala)

Resilient routing protocols aim to maintain connectivity in the case of various types of failures. The approaches are manifold, reaching from making the protocol itself more robust, maintaining alternative paths to switch to, or introducing redundancy. We studied a few protocols and their evaluation to get an understanding of the different approaches and what performance properties are important.

- Detecting and preventing malicious network activities (P. Szalachowski, Warsaw University of Technology)

This talk covered some automated and adaptive methods for recognizing a possible network attack. These methods include modern firewalls, intrusion detection and prevention systems, reputations systems and authenticity verification. Furthermore, general principles of building effective detection/prevention systems were discussed. Next, the architecture of the complete security system has been presented.

- Challenges in the current Internet & building resilient services (Dr. Ali Fessi, Munich U. of Technology)

A taxonomy for challenges in the current Internet is provided (in cooperation with Prof. James Sterbenz). Moreover, Dr. Fessi presented mechanisms for building resilient network services. Basic resilience metrics, such as service availability and reliability, are the starting point and can be considered as requirements for resilient services. Then, a variety of mechanisms was presented to fulfill these requirements, starting from simple setups with a master and a backup server, to highly distributed Peer-to-Peer (P2P) networks. Further mechanisms were discussed such as overload protection, protection against Denial-of-Service attacks, integrity protection with DNSSEC, BGP security, etc.

- Virtualization and resilience (A. Fischer, U. of Passau)

Virtualization has become popular as a method to consolidate resources and introduced an additional level of flexibility. This talk discussed the relationship of virtualization and resilience from two different perspectives. On the one hand, virtualization can be used as a mechanism to achieve or increase resilience. On the other hand, the resilience of virtualization itself was investigated.

- Exercises - Coordinator: Dr. Paul Smith (Lancaster U.)

Over the first two days of the workshop, the students designed, implemented and evaluated a piece of resilience functionality. The implementation aspect of the exercise was carried out using OpenFlow.

- Session 1: Introduction to the exercises, OpenFlow, and the basics of writing an OpenFlow controller using NOX.
- Session 2: Design, development and evaluation of the resilience functionality.

## 6. Workshop on network resilience

The research community has developed elaborate mechanisms and strategies to ensure the resilience of critical networking infrastructures. A challenge for researchers is ensuring their output is relevant to practitioners, and can thus lead to the improved resilience of current and future network deployments. This is difficult for several reasons: the challenges of acquiring useful detailed information regarding network outages; the difficulties of wide-scale experimentation with network disruptions such as attacks; the general lack of transparency regarding the challenges faced by network operators and the processes used to mitigate them; and the difficulty of modelling the complex manner in which socio-technical networked systems fail.

To contribute towards a solution, we<sup>1</sup> have organized a workshop [WNR] hosted by the 30<sup>th</sup> IEEE Symposium on Reliable Distributed Systems 2011 (SRDS), on October 4, 2011 at the Escuela Técnica Superior de Ingenieros de Minas of the Universidad Politécnica de Madrid (Spain). This workshop aimed to bring together practitioners at the frontline of providing resilient network infrastructures with the research community in order to engage in a dialogue that can steer future resilience research in directions that will meet the resilience problems of current and future networks. In line with this goal, this workshop featured a hybrid approach of individual presentations, combined with an interactive session intended to stimulate active exchange and collaboration between the communities.

We managed to produce a conference program of 5 conference presentation, 2 from academia and 3 from industry. The workshop was attended by 15 participants, about a 50%-50% split between industry and academia and managed to achieve a lively discussion between the two groups. There was a demand to possibly continue this event in the next year. The proceedings were published with IEEE, under the umbrella of the SRDS.

The program of this workshop was the following.

**Keynote:** Resilience and interconnection – scratching the surface (C. Hall, Highwayman Associates)

At the heart of the Internet is the system of connections between Internet networks. That system is generally assumed to be resilient — after all, the Internet was “designed to survive a nuclear war”. Furthermore, disasters — natural and unnatural — come and go, but the Internet seems to cope well. But, nothing this important should simply be assumed, and a closer look reveals some interesting issues about the Internet in particular, and, perhaps, about resilience in general.

### Technical session

- Wide-area virtual machine migration as resilience mechanism (A. Fischer, A. Fessi, G. Carle and H. De Meer)

The resilience of services in the Internet has become an important issue and is expected to become even more important in the future. Virtualization is one of the means which can be deployed for resilience purposes. In this paper we follow a systematic approach to the use of virtualization to increase the resilience of network services. First, we provide an analysis of the potential failures of services running

---

<sup>1</sup> C. Doerr (TU Delft), C. Rohner (Uppsala U.), M. Schöller (NEC), P. Smith (Lancaster U.), M. Karaliopoulos (National & Kapodistrian U. of Athens)

within Virtual Machines (VM) and how VM migration or replication can be used to address these failures. Then, we address the problem of re-establishing connectivity between a service and its clients upon successful migration, by leveraging results from mobility research. A special focus is given to wide-area VM migration, since it is considered as the solution for some difficult failures, e.g., large-scale failures due to natural disasters.

- Route lookup optimization including energy efficient conditions in an optical transmission network (M. Luz Mouronte, L. Luisa Vargas and P. Martínez)

The intended objective of this work is the route lookup optimization in a data transmission network taking into account its structure (deployed elements and their features), its technological characteristics (including boundary conditions, especially the energy cost of the elements belonging to the route with the best energy efficient path). This optimization also will be carried out in terms of time reduction, so it has a practical application in network management, contributing to obtain more resilient networks.

- On the benefit of network coding for timely and reliable event dissemination in WAN (C. Esposito, S. Russo, R. Beraldi and M. Platania)

Many interoperable software systems atop of large-scale critical infrastructures are based on the publish/subscribe paradigm. They are developed using data dissemination middleware services, which are required to provide reliability and timeliness in multicast communications. The literature of event dissemination and the market of publish/subscribe middleware technologies are rich of solutions, however, they hardly achieve the goal of providing fault-tolerance without violating the timeliness requirements. In this paper we present an analysis of the related work on this topic and propose an approach for combining two different approaches, namely coding and gossiping, able to satisfy timeliness and reliability requirements, respectively. We evaluate the potential benefit of coding on the information delivery performance, even when the sender introduces a redundancy to improve reliability.

- Attack resistant network embeddings for darknets (B. Schiller, S. Roos, A. Höfer and T. Strufe)

Darknets, connecting only devices between participants of mutual trust in the real world, rely on cooperative, precise, and attack resistant embeddings to evolve routing structures on the name space. Only precise embeddings allow for performant communication with low overhead on these networks. With Darknets being deployed in generally untrusted, even adverse environments, external or internal attacks have to be assumed commonplace. Their impact hence has to be limited and the embedding must be made resistant against even sophisticated attacks. Analysing Dark Freenet, the only current approach implementing a full Dark net, we devise simple attacks that render its embedding entirely corrupt. In response we derive a novel embedding that is based on local decisions only, and which not only is resistant to such attacks, but additionally outperforms the Dark Freenet in terms of precision.

- Distributed fault diagnosis using bayesian reasoning in MAGNETO (P. Arozarena, R. Toribio and A. Carrera)

Many of the emerging telecom services make use of Outer Edge Networks, in particular Home Area Networks. The configuration and maintenance of such services may not be under full control of the telecom operator which still needs to guarantee the service quality experienced by the consumer. Diagnosing service faults in these scenarios becomes especially difficult since there may be not full visibility between different domains. This paper describes the fault diagnosis solution developed in the MAGNETO project, based on the application of Bayesian Inference to deal with the uncertainty. It also takes advantage of a distributed framework to deploy diagnosis components in the different domains and network elements involved, spanning both the telecom operator and the Outer Edge networks. In addition, MAGNETO features self-learning capabilities to automatically improve diagnosis knowledge over time and a partition mechanism that allows breaking down the overall diagnosis knowledge into smaller subsets. The MAGNETO solution has been prototyped and adapted to a particular outer edge scenario, and has been

further validated on a real testbed. Evaluation of the results shows the potential of our approach to deal with fault management of outer edge networks.

**Discussion session:** WNR discussion session ideas

**Concluding remarks**

## 7. Further impact

Another aspect of dissemination work is constituted by liaison activities with other FP7 projects. ResumeNet has filled a questionnaire launched by UniverSelf ([www.univerself-project.eu](http://www.univerself-project.eu)) in November 2010, as well as a description of our objectives and results has been provided to some partners of this project launched recently, for its potential applicability to autonomics for future networks. A half-day common meeting was organized on February 3rd 2011 in Liège (Belgium) with ECODE ([www.ecode-project.eu](http://www.ecode-project.eu)), during which partners from each consortium have presented their respective work which could be potentially interesting for the other project.

As mentioned in a previous project periodic report (D6.4d), ENISA, the European Network and Information Security Agency, has invited ResumeNet to present its work during their 1st Workshop on "Network and service resilience metrics and measurement frameworks". This event was held in Brussels (Belgium) on December 1st 2010. Representing the consortium, Dr. Christian Doerr (TU Delft) has described ResumeNet results and the metrics work done in WP1. As a lot of attention was generated by the assistance for the project, ENISA is seeking for further collaboration.

Within the IU-ATC project ([www.iu-atc.com](http://www.iu-atc.com)), Lancaster University (UK) leads, together with IIT Madras (India), the theme 4 on "Security and resilience monitoring for NGNs"<sup>2</sup>. Within this theme, a distributed measurement and control system to detect the onset and remediate the effects of abnormal network behaviour is designed. Further, the potential of cross-layer synergy between the application and the network layers, and the correlation of temporal performance metrics at different points in the network (routers, hosts) to provide fast detection and recovery is investigated. The detection mechanism is based on real-time analysis of traffic arrival rate at different points in the network and the way this is aggregated towards the target(s), using control-theoretic approaches. Appropriate remediation strategies are also developed for different classes of anomalies detected. The impact of efficient information exchange between the infrastructure and the application layers, and the combination of local and remote control enforcement for fast remediation are studied. Another point of investigation is the use of policies in the context of the  $D^2R^2+DR$  control loop and autonomic network management for resilient networks.

Lancaster U. has collaborated with British Telecom within the context of IU-ATC on more end-system specific issues related to cyber security and resilience. In this framework, two joint studentships in the area of "Malware detection and prevention based on application-specific behavioural monitoring", and "Adaptive intrusion detection systems" were launched.

We have also mentioned in D6.4d the visit of Prof. David Hutchison from Lancaster U. planned for the end of 2010 in Australia. This visit took place in December 2010, and provided an opportunity to present the latest work in ResumeNet to the Military Communications research group at the Defence Science and Technology Organisation (DSTO) in Adelaide. Significant interest was raised through the discussion, leading to an agreement of the two groups to maintain contact.

---

<sup>2</sup> Three other partners of this theme are U. of Ulster, BT and NMS Works

Dr Mixia Liu from the Lanzhou University of Technology (China) came to Lancaster University as a visiting researcher for a year, until the beginning of December 2011. During her visit, she investigated how models of situational awareness can be applied and extended to the process of determining the nature of a challenge for network resilience. This investigation proved very useful for understanding the process of challenge detection, with respect to the  $D^2R^2+DR$  resilience strategy, and how better decisions can be made about remediation. Her work resulted in a publication being accepted at a symposium in Liverpool, UK, and a paper was also submitted to a conference to be held in China, the outcome of which we will learn of in the New Year.

Finally, colleagues at Lancaster University have filed a patent on on-going work about a novel approach to the on-line identification and mitigation of network flows that are understood to be part of a botnet, e.g., its command and control traffic. This work will form part of Radovan Bruncak's PhD contribution, who is expected to submit his thesis in 2012 (see D5.3b "Exploitation plans (final)").

## **8. Contribution to standardization work**

ResumeNet's contribution to the "Focus Group on Future Networks", issued from the study group 13 of ITU-T, is included in the final document entitled "Draft Deliverable on Future Networks: Objectives and Design Goals" (reference: TD-WP5-132).

Dr. Marcus Schöller from NEC (Germany) has also contributed to another ITU publication entitled "Project descriptions on Future Networks" (reference: TD-WP5-104).

In the MME restoration work [TAL], we proposed a proactive restoration approach that proactively triggers MME relocation and restoration of lost state to avoid service disruption at a later stage. This approach addresses UEs in both idle and active mode. For the former, it triggers all affected idle-mode UEs through "scheduled/randomized bulk paging" to re-attach to the network. As for the latter, it allows ongoing communications to proceed and triggers affected UEs to perform a Tracking Area Update (TAU) in a scheduled manner according to predefined priorities. Both mechanisms lead to the selection of a new MME for affected UEs and restoration of their context in a pro-active manner. Based on these research results, NEC has contributed two work items to 3GPP's SA2: Core Network Overload [CNO] and Network Improvement for Machine Type Communications [NIMTC]. Both were appreciated by 3GPP, but seen as implementation matter to be addressed by CT instead of SA. A continuation of this activity has not been decided yet.

## References

- [CNO] [www.3gpp.org/ftp/Specs/html-info/23843.htm](http://www.3gpp.org/ftp/Specs/html-info/23843.htm)
- [DoW] ResumeNet, "Description of work", 7th Framework Programme, Theme ICT-2007.1.6, New paradigms and experimental facilities, Grant agreement n° 224619, March 2008
- [ENF] [euronf.enst.fr](http://euronf.enst.fr)
- [NIMTC] [www.3gpp.org/ftp/Specs/html-info/23888.htm](http://www.3gpp.org/ftp/Specs/html-info/23888.htm)
- [RES] [www.resumenet.eu/course/index](http://www.resumenet.eu/course/index)
- [SRDS] [lsd.ls.fi.upm.es:11888/srds](http://lsd.ls.fi.upm.es:11888/srds)
- [TAL] T. Taleb, and K. Samdanis, "Ensuring service resilience in the EPS: MME failure restoration case", IEEE Globecom 2011, Houston, Texas, USA, December 5-9 2011
- [WNR] [www-nas.et.tudelft.nl/wnr](http://www-nas.et.tudelft.nl/wnr)



## Annex

This annex resumes the ResumeNet publications realized during the first two years of the project.

### Magazines

- D. Hutchison, and J.P.G. Sterbenz, "*ResiliNets: resilient and survivable networks*," ERCIM News 77, April 2009
- A. Berl, A. Fischer, and H. de Meer, "Virtualization in the future Internet - virtualization methods and applications", Informatik Spektrum - Issue on Future Internet, Vol. 33, N° 2, Springer-Verlag, April 2010, pp. 186-194 (in German)
- N. Kammenhuber, A. Fessi, and G. Carle, "Resilience of the Internet against disruptions - state of the art in R&D", Informatik Spektrum - Issue on Future Internet, Vol. 33, N° 2, Springer-Verlag, April 2010, pp. 131-142 (in German)

### Journals

- A. Feldmann, S. Fischer, N. Kammenhuber, and B. Vöcking, "*Management of variable data streams in networks*," in 'Algorithmics of Large and Complex Networks' (J. Lerner, D. Wagner, and K. Zweig, Eds.), Lecture Notes in Computer Science, Volume 5515, Springer Verlag, 2009
- P. Van Mieghem, J. Omic, and R. Kooij, "*Virus spread in networks*", IEEE/ACM Transactions on Networking, Vol. 17, No. 1, February 2009, pp. 1-14
- M. Karaliopoulos, "Assessing the vulnerability of DTN data relaying schemes to node selfishness", IEEE Communication Letters, Vol. 13, N° 12, December 2009, pp. 923-925
- M. Sifalakis, M. Fry, and D. Hutchison, "Event detection and correlation for network environments", IEEE Journal on Selected Areas in Communications - Special issue on "Recent Advances in Autonomic Communications", Vol. 28, N° 1, January 2010, pp. 60-69
- T. Taleb, and K. Ben Letaief, "A cooperative diversity based handoff management scheme", IEEE Transactions on Wireless Communications, Vol. 9, N° 4, April 2010, pp. 1462-1471
- J.P.G. Sterbenz, D. Hutchison, E.G. Cetinkaya, A. Jabbar, J.P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: strategies, principles, and survey of disciplines", Computer Networks - Special Issue on Resilient and Survivable Networks, Elsevier, Vol. 54, N° 8, June 2010, pp. 1245-1265
- Z. Fadlullah, T. Taleb, M. Guizani, and N. Kato, "DTRAB: Combating against attacks on encrypted protocols through traffic-feature analysis", IEEE/ACM Transactions on Networking, Vol. 18, N° 4, August 2010, pp. 1234-1247

### Conferences and workshops

- A. Jabbar, J.P. Rohrer, A. Oberthaler, E.K. Çetinkaya, V.S. Frost, and J.P.G. Sterbenz, "*Performance comparison of weather disruption-tolerant cross-layer routing algorithms*", in Proc. of 28th IEEE Conference on Computer Communications (INFOCOM), Rio de Janeiro, Brazil, April 19-25, 2009
- J. Omic, A. Orda, and P. Van Mieghem, "*Protecting against network infections: a game theoretic perspective*", in Proc. of IEEE 28th IEEE Conference on Computer Communications (INFOCOM), Rio de Janeiro, Brazil, April 19-25, 2009
- J. Omic, R. E. Kooij, and P. Van Mieghem, "*Heterogeneous protection in regular and complete bi-partite networks*", in Proc. of IFIP Networking, Aachen, Germany, May 11-15, 2009
- N. Kammenhuber, "*Dynamic traffic engineering in the future (?) Internet*", in Proc. of 3rd GI-ITG/KuVS Workshop on the Future Internet, Munich, May 28<sup>th</sup>, 2009

- Z. Fadlullah, T. Taleb, N. Nasser, and N. Kato, "*Exploring the security requirements for quality of service in combined wired and wireless networks*", in Proc. of ACM IWCMC'09, Leipzig, Germany, June 21-24, 2009
- R. Bruncak, P. Smith, D. Hutchison, and J. P.G. Sterbenz, "Towards multilevel resilience for future networking," in Proc. of 10th Annual Postgraduate Symposium on The Convergence of Telecommunications, Networking & Broadcasting (PGNet), Liverpool, UK, June 22-23, 2009
- N. Kheir, H. Debar, N. Cuppens-Bouahia, F. Cuppens, and J. Viinikka, "*Cost evaluation for intrusion response using dependency graphs*", in Proc. of IFIP International Conference on Networks and Service Security (N2S), Paris, France, June 24-26, 2009
- N. Kheir, H. Debar, F. Cuppens, N. Cuppens-Bouahia, and J. Viinikka, "*A service dependency modelling framework for policy-based response enforcement*", in Proc. of DIMVA, Milan, Italy, July 9-10, 2009
- M. Schöller, T. Taleb, and S. Schmid, "Neighbourhoods as an abstraction for fish-eye state routing", IEEE PIMRC, Tokyo, Japan, September 13-16, 2009
- A.A. Beshir, F.A. Kuipers, A. Orda, and P. Van Mieghem, "On-line survivable routing in WDM networks", 21st International Teletraffic Congress (ITC 21), Paris, France, September 15-17, 2009
- F. Hugelshofer, P. Smith, D. Hutchison, and N.J.P. Race, "OpenLIDS: a lightweight intrusion detection system for wireless mesh networks", 15th Annual International Conference on Mobile Computing and Networking (MobiCom), Beijing, China, September 20-25, 2009
- J.P. Rohrer, R. Naidu, and J.P.G. Sterbenz, "Multipath at the transport layer: an end-to-end resilience mechanism", International Workshop on Reliable Networks Design and Modelling (RNDM), St. Petersburg, Russia, October 12-14, 2009
- T. Taleb, Z. Fadlullah, M. Schöller, and K. Letaif, "A connection stability aware mobility management scheme", IEEE WiMOB, Marrakech, Morocco, October 12-14, 2009
- J.P. Rohrer, A. Jabbar, and J.P.G. Sterbenz, "Path diversification: a multipath resilience mechanism", 7th IEEE International Workshop on the Design of Reliable Communication Networks (DRCN), Washington, DC, USA, October 25-28, 2009
- C. Auer, P. Wüchner, and H. de Meer, "The degree of global-state awareness in self-organizing systems", International Workshop on Self-Organizing Systems (IWSOS), Zürich, Switzerland, December 9-11, 2009
- C. Doerr, P. Smith, and D. Hutchison, "Network heterogeneity and cascading failures - an evaluation for the case of BGP vulnerability", International Workshop on Self-Organizing Systems (IWSOS), Zürich, Switzerland, December 9-11, 2009
- W. Elmenreich, R. D'Souza, Ch. Bettstetter, and H. de Meer, "A survey of models and design methods for self-organizing networked systems", International Workshop on Self-Organizing Systems (IWSOS), Zürich, Switzerland, December 9-11, 2009
- R. Holzer, and H. de Meer, "Quantitative modelling of self-organizing properties", International Workshop on Self-Organizing Systems (IWSOS), Zürich, Switzerland, December 9-11, 2009
- E. Gourdin, "A mixed-integer model for the sparsest cut problem", ISCO 2010, Hammamet, Tunisia, March 24-26, 2010
- J.P.G. Sterbenz et al., "The Great Plains Environment for Network Innovation (GpENI): a programmable testbed for future Internet architecture research", 6th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (TridentCom), Berlin, Germany, May 18-20, 2010
- M. Fry, M. Fischer, M. Karaliopoulos, P. Smith, and D. Hutchison, "Challenge identification for network resilience", NGI 2010, Paris, France, June 2-4, 2010
- G. Popa, E. Gourdin, F. Legendre, and M. Karaliopoulos, "On maximizing collaboration in wireless mesh networks without monetary incentives", RAWNET - Resource Allocation in Wireless Networks (with WiOpt 2010), Avignon, France, June 4, 2010
- J. Lessmann, M. Schöller, F. Zdarsky, and A. Banchs, "Rope ladder routing: position-based multipath routing for wireless mesh networks", 2nd IEEE WoWMoM Workshop on Hot Topics in Mesh Networking, Montreal, Canada, June 10-17, 2010

- M. Schöller, P. Smith, C. Rohner, M. Karaliopoulos, A. Jabbar, J.P.G. Sterbenz, and D. Hutchison, "On realising a strategy for resilience in opportunistic networks", Future Network and Mobile Summit, Florence, Italy, June 16-18, 2010
- P. Smith, A. Schaeffer-Filho, A. Ali, M. Schöller, N. Kheir, A. Mauthe, and D. Hutchison, "Strategies for network resilience: capitalising on policies", AIMS 2010, Zürich, Switzerland, June 21-25, 2010
- C. Doerr, and J. Martin-Hernandez, "A computational approach to multi-level analysis of network resilience", DEPEND 2010, Venice, Italy, July 18-25, 2010
- A. Fessi, N. Evans, H. Niedermayer, and R. Holz, "Pr2-P2PSIP: privacy preserving P2P signalling for VoIP and IM", Principles, Systems & Applications of IP Telecommunications (IPTComm), Munich, Germany, August 2-3, 2010

## Presentations

- B. Plattner, "*Resilience and survivability for future networking: framework, mechanisms, and experimental evaluation*", SAC-FIRE Workshop, Turin, Italy, March 5th 2008
- B. Plattner, "*FP7 ResumeNet STREP - Resilience and survivability for future networking: framework, mechanisms, and experimental evaluation*", The Future of the Internet, Bled, Slovenia, April 2nd 2008
- D. Hutchison and C. Edwards, "*QoS: (still) a grand challenge?*", Invited talk at IWQoS 2008, Twente, Netherlands, June 3<sup>rd</sup> 2008
- M. Karaliopoulos, "*ResumeNet*", Poster presented at FIRE launch event, Paris, France, September 10<sup>th</sup> 2008
- P. Smith and D. Hutchison, "*Towards resilient networked systems with self-organizing mechanisms*", Abstract presented at IWSOS, Vienna, Austria, December 10-12, 2008
- J.P.G. Sterbenz, "*Dynamic and adaptive architectures for network resilience*", Keynote address at 2nd ICC Winter Workshop on Complexity in Social Sciences, Lisboa, Portugal, January 10th 2009
- B. Plattner, "*Resilience and survivability for future networking: framework, mechanisms, and experimental evaluation*", NetArch Symposium (on the 40<sup>th</sup> Anniversary of the 1st RFC), Monte Verità - Ascona, Switzerland, March 16-19, 2009
- G. Popa, "*Analytically estimating the impact of node misbehaviors on the throughput of wireless multihop networks*", Perspectives Workshop: Architecture and Design of the Future Internet, Dagstuhl Seminar, Germany, April 13-17, 2009
- M. Schöller, "*Understanding challenges and their impact on network resilience*", Perspectives Workshop: Architecture and Design of the Future Internet, Dagstuhl Seminar, Germany, April 13-17, 2009
- B. Plattner, "*How good is the future Internet ?*", Future of the Internet Conference, Prague, Czech Republic, May 11-13, 2009
- J.P.G. Sterbenz, D. Hutchison, A. Jabbar, J.P. Rohrer, and E. Çetinkaya, "*Resilience, survivability, and heterogeneity in the postmodern Internet*", Invited presentation at the 4th International Conference on Future Internet Technologies, Seoul, June 17-19, 2009
- P. Smith, M. Schoeller, and D. Hutchison, "*Understanding risk for network resilience*", Multi-Service Networks, Abingdon, UK, July 9-10, 2009
- J.P.G. Sterbenz, D. Hutchison, B. Plattner, D. Medhi, B. Ramamurthy, C. Scoglio, A. Jabbar, J. P. Rohrer, and E. Çetinkaya, "*Postmodern resilience and international collaboration in GpENI*", Multi-Service Networks, Abingdon, UK, July 9-10, 2009
- J.P.G. Sterbenz, D. Hutchison, B. Plattner, D. Medhi, B. Ramamurthy, and C. Scoglio, "*GpENI and ResiliNets: international collaboration in GENI, FIND, and FIRE*", Invited talk at the 2nd GENI-FIRE Workshop, Seattle, WA, USA, July 13th 2009
- A. Fischer, A. Berl, A. Galis, and H. de Meer, "Network virtualization in AutoI and ResumeNet", Future Internet Cluster Meeting, Sophia Antipolis, France, 9th March 2010
- J.P.G. Sterbenz, D. Hutchison, P. Smith, E.K. Çetinkaya, M. Hameed, A. Jabbar, and J.P. Rohrer, "Evaluation of network resilience: analysis, simulation, and experimentation", Multi-Service Networks, Abingdon, UK, July 8-9, 2010

Download link: [www.resumenet.eu/results/presentations](http://www.resumenet.eu/results/presentations)

## **Publicity**

- B. Plattner, "Internet 2.0 - Renovation oder Neubau?", Neue Zürcher Zeitung, March 2009 (in German)
- B. Plattner, "The future of the Internet", ETH Life, September 2009 (in German)

Download link: [www.resumenet.eu/results/publicity](http://www.resumenet.eu/results/publicity)