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

Deliverable number:	D5.2b
Deliverable name:	Second Year Report on Dissemination Activities
WP number:	5
Delivery date:	31.08.2010
Date of preparation:	20.09.2010
Editor:	C. Lac (FT)
Contributors:	C. Doerr (TUD), A. Fessi (TUM), A. Fischer (UP), M. Fry (USyd), E. Gourdin (FT), D. Hutchison (ULanc), C. Lac (FT), G. Popa (ETHZ), M. Schöller (NEC), P. Smith (ULanc), J.P.G. Sterbenz (KU), T. Taleb (NEC)
Internal reviewers:	D. Hutchison (ULanc), M. Karaliopoulos (ETHZ)

Summary

This deliverable reports on the different dissemination and standardization activities carried out during the second year of the ResumeNet 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 conferences and journals of the field;
- the project presentations in symposia organized by European Commission related Actions;
- the use of additional communication channels (e.g., university magazines, interviews, poster presentations) to publicize the concepts and objectives of the project;
- the continuation of collaboration with institutions carrying out resilience-related activities in Europe, US, and Pacific region;
- the contribution of ResumeNet to the "Focus Group on Future Networks", a focus group constituted in 2009 by the Study Group 13 ("Future networks including mobile and NGN") of the International Telecom Union's standardization sector (IUT-T).

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. Magazines 2
2.2. Journals 2
2.3. Conferences and workshops 4
2.4. Ongoing work 11
3. Presentations 13
4. Publicity 13
5. Further impact 14
6. Contribution to standardization work 15
References 16

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) in October 2008.

A major revision of the site's pages was realized in July 2009. As described in last year's report on dissemination activities [D5_2a], 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 download 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 2: 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*".

Research work carried out since the start of the project in September 2008 has been submitted, and, in most cases, accepted and published, to scientific conferences/workshops, journals, or magazines. The full set of publications/submissions covering the second year of the project is listed below, followed by a short description of their contents and their links to ResumeNet.

2.1. Magazines

"Informatik-Spektrum" is a scientific magazine in German published every two months by the organization "Gesellschaft für Informatik (GI)". GI has more than 20,000 members mainly from academia. The audience is thus much larger than the Computer Networks community. Prof. Thorsten Braun (University of Bern) edited a special issue on Future Internet in "Informatik-Spektrum" of April 2010. The ResumeNet consortium contributed with two articles to this special issue.

● 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)

The Future Internet architecture has to overcome ossification and shortcomings of the current Internet. It has to be robust, reliable, and fault tolerant, for instance, and it has to provide services in energy efficient ways. Furthermore, it is necessary to anticipate demands made by future services and networks, in order to enable the development of new services and protocols. Such goals require a highly flexible and reconfigurable network architecture, including simple and autonomous network management. Virtualization of host and network resources is among the key technologies in this context to achieve the needed flexibility. Virtualization is able to hide the complexity of physical network infrastructures and to provide homogenous, flexible, and dynamically reconfigurable virtual resources instead. This paper gives an overview on different methods of host and network virtualization. It illustrates (based on several examples) how challenges and requirements of today's Internet as well as those of the Future Internet can be approached. With regard to ResumeNet, this paper points out how to use virtualization mechanisms in order to increase the resilience of network services.

● 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)

Although today's Internet operates remarkably well, it cannot be considered as resilient. One of the reasons is the fact that the requirements at the time when the Net was developed have since evolved significantly. In this article, we first discuss the notion of 'resilience'. Then we describe the weak points of today's Internet. The main contribution of this paper is a broad overview on network resilience technologies that are either already in use in today's Internet, or that are being developed or about to be deployed in the mid to near future. The paper supports the rationale for, as well as the importance of, the ResumeNet project.

2.2. Journals

● 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

This letter analytically assesses the vulnerability of two popular data relaying alternatives, the unrestricted and two-hop relay schemes, to node selfishness. Network nodes may behave selfishly often due to some resource preservation policy, in particular when they are constrained with respect to energy or/and storage space. The results suggest that the performance advantage of unrestricted relaying over two-hop relaying decreases both with the number of selfish nodes and the intensity of their selfishness, irrespective of whether nodes defer from relaying deterministically or probabilistically. The proposed model can be used to quantify the vulnerability of the two relaying schemes to node selfishness but also drive remediation actions against it. This work feeds into task 1.2 of ResumeNet, where a risk assessment approach has been introduced for assessing the impact of several challenges to network normal operation. Analytical modelling is one of the ways to obtain hints about the actual performance degradation due to challenges, in particular

when measurement data are hard to obtain. The challenge addressed in this paper is the node selfishness and the network scenario corresponds to the second case study of the project, which is subject of experimentation in WP4.

● 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

Networks with desirable self-* properties should be more adaptable to changing conditions and would enable greater flexibility and functional scalability to support resilient operation. A necessary condition for realising these benefits is a heightened level of network awareness; this requires not merely the capacity to monitor the system and network state, but also the ability to characterise the operational environment and its dynamic shifts. This article presents the design framework and initial evaluation of an Information Sensing system that aims to enable awareness through an integrated event detection-correlation mechanism. In the context of systems resilience, it can be used for operational awareness and it offers a more lightweight solution than traditional active database-oriented event systems. It has better performance than log-post analysis processing and its design enables a distributed detection facility. This is fundamental for network-level context awareness and for leveraging decision making and respective action taking, with regard to resilient operation as planned in ResumeNet.

● 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

Cooperative diversity has emerged as a promising technique to facilitate fast handoff mechanisms in mobile ad-hoc environments. The key concept behind a prominent cooperative diversity based protocol, namely, Partner-based Hierarchical Mobile IPv6 (PHMIPv6), is to enable mobile nodes anticipate handover events by selecting suitable partners to communicate on their behalves with Mobility Anchor Points (MAPs). In the original design of PHMIPv6, mobile hosts choose partners based on their signal strength. Such a naive selection procedure may lead to scenarios where mobile hosts lose communication with the selected partners before the completion of the handoff operations. In addition, PHMIPv6 overlooks security considerations, which can easily lead to vulnerable mobile hosts and/or partner entities. As a solution to these two shortcomings of PHMIPv6, this paper first proposes an extended version of PHMIPv6 called Connection Stability Aware PHMIPv6 (CSA-PHMIPv6). In CSA-PHMIPv6, mobile hosts select partners with whom communication can last for a sufficiently long time by employing the Link Expiration Time (LET) parameter. To tackle the security issues, the simple yet effective use of two distinct authentication keys is envisioned. Furthermore, to shorten the communication time between mobile hosts and their corresponding partners, a second handoff management approach called Partner Less Dependable PHMIPv6 (PLD-PHMIPv6) is proposed. This paper adds the flavour of resiliency, one of the key aspects of the ResumeNet project, to the partner-based HMIPv6 protocol via a resiliency-aware selection of partners. The paper also addresses some security flaws with the original design of the protocol.

● 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

The Internet has become essential to all aspects of modern life, and thus the consequences of network disruption have become increasingly severe. It is widely recognised that the Internet is not sufficiently resilient, survivable, and dependable, and that significant research, development, and engineering is necessary to improve the situation. This paper provides an architectural framework for resilience and survivability in communication networks and provides a survey of the disciplines that resilience encompasses, along with significant past failures of the network infrastructure. A resilience strategy is presented to defend against, detect, and remediate challenges, a set of principles for designing resilient

networks is presented, and techniques are described to analyse network resilience. This strategy was at the heart of the original ResumeNet project proposal, and is the basis for the project objectives as well as the work package structure. In particular, ResumeNet's WP1 is assessing the applicability of the D^2R^2+DR approach for building resilient networks. This paper presents the up-to-date strategy, and acts as a framework paper for the ResumeNet project.

● 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

The unbridled growth of the Internet and the many and varied network-based applications have contributed to enormous security leaks. Even the cryptographic protocols, which are used to provide secure communications, are often targeted by diverse attacks. Intrusion Detection Systems (IDSs) are often employed to monitor network-traffic and host-activities which may lead to unauthorized accesses and attacks against vulnerable services. Most of the conventional misuse-based and anomaly-based IDSs are ineffective against attacks targeted at encrypted protocols since they heavily rely on inspecting the payload-contents. To combat against attacks on encrypted protocols, an anomaly based detection system using strategically distributed Monitoring Stubs (MSs) is proposed. Various attacks against cryptographic protocols have been categorized. The MSs, by sniffing the encrypted traffic, extract features for detecting these attacks and construct normal usage behaviour profiles. Upon detecting suspicious activities due to the deviations from these normal profiles, the MSs notify the victim servers, which may then take necessary actions. In addition to detecting attacks, the MSs can also trace back the originating network of the attack. This unique approach is called DTRAB, since it focuses on both detection and trace back in the MS level. The effectiveness of the proposed detection and trace back methods are verified through extensive simulations and Internet datasets. The work described in this paper fits well with tasks 2.2 and 2.3 of the ResumeNet project.

2.3. Conferences and workshops

● M. Schöller, T. Taleb, and S. Schmid, "Neighbourhoods as an abstraction for fish-eye state routing", IEEE PIMRC, Tokyo, Japan, September 13-16, 2009

This paper presents a routing scheme based on metric dependent neighbourhoods to calculate the forwarding graph. The proposed routing scheme supports aggregation of this metric related information while disseminating routing updates to retain scalability. Simulation results with an exemplary metric based on link stability information show the feasibility of this aggregation approach and the improvement with respect to node reachability and reliable communication in self-organizing wireless networks. In the framework of ResumeNet, this routing algorithm can be used as a resilient routing component in ad-hoc wireless networks.

● 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

Wireless mesh networks (WMNs) are being used to provide Internet access in a cost efficient manner. Typically, consumer-level wireless access points with modified software are used to route traffic to potentially multiple back-haul points. Malware infected computers generate malicious traffic, which uses valuable network resources and puts other systems at risk. Intrusion detection systems can be used to detect such activity. Cost constraints and the decentralised nature of WMNs make performing intrusion detection on mesh devices desirable. However, these devices are typically resource constrained. This paper describes the results of examining their ability to perform intrusion detection. Our experimental study shows that commonly-used deep packet inspection approaches are unreliable on such hardware. A set of lightweight anomaly detection mechanisms as part of an Intrusion Detection System (IDS), called OpenLIDS is implemented. It is shown that, even with the limited hardware resources of a mesh device, it

can detect current malware behaviour in an efficient way. This paper relates to Task 2.2 on challenge detection, and introduces some of the constraints of performing intrusion detection in multi-hop wireless mesh networks, as investigated in WP4. The results can be used as a basis for further work on distributed challenge detection, as one may view OpenLIDS as a component of a larger distributed detection system that looks at specific challenges, i.e., attacks, at certain layers of the protocol stack.

● 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

As society's dependence on network technology increases, the need for resilience and survivability in these services becomes increasingly apparent. Since the user experience is ultimately determined by the dependability of the end-to-end service, the transport layer is one area where this issue can be addressed. This paper introduces a resilient multipath selection algorithm, which obtains multiple end-to-end paths in the WAN context through cross-layer interaction with lower layers of the network. This cross-layer interface is provided by a thin internetwork protocol (PoMo), which supports heterogeneity at trust and policy boundaries. The result is a more resilient end-to-end service provided to applications by taking advantage of redundancy in the underlying physical network. The efficiency tradeoffs of the multipath approach is evaluated on two topologies, a synthetic one and one corresponding to a tier 1 ISP's backbone network. This paper applies ResumeNet design principles of redundancy, diversity, and cross-layering to network and transport protocol design.

● T. Taleb, Z. Fadlullah, M. Schöller, and K. Letaif, "A connection stability aware mobility management scheme", IEEE WiMOB, Marrakech, Morocco, October 12-14, 2009

Exploiting the cooperative diversity paradigm in Partner-based Hierarchical MIPv6 (PHMIPv6) promises an acceleration of the handoff management operation by relaying some signalling over a selected partner node prior to the actual handover to the new access point. For this purpose, a suitable partner node that stays in communication range for sufficient time until the signalling in the pre-handoff phase is finalized, should be selected. This paper shows that using the Link Expiration Time (LET) metric to select the partner node can significantly improve handovers in Mobile IP (MIP) networks. The basis of this new metric is the relative position and the relative speed of the mobile node to the potential partner nodes. The presented algorithm features a node selection algorithm for reliable communication for hand-off preparation. Mechanisms to be proposed in WP2 and WP3 should benefit from such a cooperative behaviour, seen as a fundamental principle for resilient networking.

● 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

Path diversification is a new mechanism that can be used to select multiple paths between a single ingress and egress node pairs using a quantified diversity measure to achieve maximum flow reliability. The path diversification mechanism is targeted at the end-to-end layer but can be applied at any level for which a path discovery service is available, e.g., intra-realm routing or inter-realm routing. Path diversification also takes into account higher level requirements for low-latency or maximal reliability in selecting appropriate paths. Using this mechanism will allow future internetworking architectures to exploit naturally rich physical topologies to a far greater extent than is possible with shortest-path routing or equal-cost load balancing. This paper describes the path diversity metric and its application at various aggregation levels. This metric is then applied to the path diversification process in the context of several real-world network graphs to assess the gain in flow reliability. This paper applies ResumeNet design principles of redundancy and diversity to network topology design.

● 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

Since the entities composing self-organizing systems have direct access only to information provided by their vicinity, it is a nontrivial task for them to determine properties of the global system state. However, this ability appears to be mandatory for certain self-organizing systems in order to achieve an intended functionality. Based on Shannon's information entropy, we introduce a formal measure that allows to determine the entities' degree of global-state awareness. Using this measure, self-organizing systems and suitable system settings can be identified that provide the necessary information to the entities for achieving the intended system functionality. Hence, the proposed degree supports the evaluation of functional properties during the design and management of self-organizing systems. We show this by applying the measure exemplarily to a self-organizing sensor network designed for intrusion detection. This allows us to find preferable system parameter settings. In this paper, resilience is proposed as one of the formal measures. To have a resilient system, it is useful for the entities of a self organizing system to know certain aspects of the system's global state.

● 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

While individual and isolated challenges may cause considerable harm inside a computer network, certain challenges might trigger chains of subsequent failures that will spread into large parts of an infrastructure and have the potential to severely affect the entire system. There have been a number of theoretical studies of complex network structures suggesting that heterogeneous networks, in terms of node connectivity and load, are more vulnerable to cascading failures than those which are more homogeneous. We describe in this paper early research into an investigation of whether this thesis holds true for vulnerabilities in the Internet's inter-domain routing protocol - BGP - in light of different network structures. We find that network homogeneity as suggested by theory does not protect the overall network from failures in practice, but instead may even be harmful to network operations. This paper was stimulated by the joint Delft-Lancaster activities in ResumeNet and contributes to the thinking within the project about the vulnerabilities of networks and how they can be overcome.

● 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

Self-organization, whereby through purely local interactions, global order and structure emerge, is studied broadly across many fields of science, economics, and engineering. We review several existing methods and modelling techniques used to understand self-organization in a general manner. We then present implementation concepts and case studies for applying these principles for the design and deployment of robust self-organizing networked systems. A combination of the presented design approaches can be useful in the system design process and will ultimately help in building a resilient system. This work was primarily planned during the Lakeside Research Days in July 2009 under the topic of resilience of self organizing systems. This work informs the thinking in ResumeNet about automated approaches to realizing resilient networks, and potentially makes a contribution to the inner and outer control loops of the D^2R^2+DR framework and in particular to whether there should always be a human in the loop. It may also inform the project's thinking about the outer Diagnose-Refine loop in which the model represented by the inner loop may be adjusted – whether autonomically or by the intervention of a human.

● 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

For analyzing properties of complex systems, a mathematical model for these systems is useful. In this paper, we give quantitative definitions of adaptivity, target orientation, homogeneity and resilience with respect to faulty nodes or attacks by intruders. The modelling of the system is done by using a multigraph to describe the connections between objects and stochastic automatons for the behaviour of the objects. The quantitative definitions of the properties can help for the analysis of existing systems and for the design of new systems. To show the practical usability of the concepts, the definitions are applied to a slot synchronization algorithm in wireless sensor networks. Since modeling and metrics in the context of ResumeNet project are required, this paper gives an overview of quantitative modeling of self-organizing properties.

● E. Gourdin, "A mixed-integer model for the sparsest cut problem", ISCO 2010, Hammamet, Tunisia, March 24-26, 2010

In a capacitated graph with a set of commodities, the sparsity of a cut is the ratio between the capacity of the cut and the demand of the commodities separated by the cut. The Sparsest Cut (SC) is often introduced as a weak dual of the Maximum Concurrent Flow problem (MCF). Contrarily to MCF, the SC problem is, in general, NP-hard. This problem has been considerably studied, motivating the design of very elaborated approximation algorithms. Somewhat surprisingly, to the best of our knowledge, the SC problem has not been investigated with exact approaches using Mixed Integer Programming models. In this paper, we propose a formulation arising "naturally" from the dual of MCF. The sparsest cut in a network is a clear indication of one of the network weaknesses. Indeed, it is the set of links that will most likely first become saturated if the traffic conditions change in an homogeneous way. Identifying such cuts is hence important to show where to focus the attention in order to increase the network robustness.

● 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

The Great Plains Environment for Network Innovation (GpENI) is an international programmable network testbed centered on a regional optical network in the Midwest US, providing flexible infrastructure across the entire protocol stack. The goal of GpENI is to build a collaborative research infrastructure enabling the community to conduct experiments in future Internet architecture. GpENI is funded in part by the US National Science Foundation GENI (Global Environments for Network Innovation) Program and by the EU FIRE (Future Internet Research and Experimentation) Programme, and is affiliated with a project funded by the NSF FIND (Future Internet Design) Program.

● M. Fry, M. Fischer, M. Karaliopoulos, P. Smith, and D. Hutchison, "Challenge identification for network resilience", NGI 2010, Paris, France, June 2-4, 2010

It is widely agreed that the Internet needs to become more resilient to a range of challenges that can seriously impact the normal operation of the network and networked services. Challenges include malicious attacks, mis-configurations, accidental faults and operational overloads. Our starting point in this paper is an overall strategy for network resilience, which draws on existing or under development mechanisms that can be used to maintain acceptable levels of operation in the event of challenges. A crucial part of this strategy is the identification of challenges in real-time, followed by the application of appropriate remedial action. In this paper, we motivate and describe a new approach to challenge identification that goes beyond current techniques for attack, anomaly or fault detection. We describe our proposed approach in the context of known network challenge scenarios and identify the gaps in the state of the art that our work is filling. We indicate its validity by showing how it can address the challenge of interference in wireless mesh networks. The paper details the requirements of the challenge detection stage of the ResumeNet strategy and applies it to a known challenge scenario as validation. It reports ongoing work in Task 2.2.

● 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

In distributed network settings, where nodes are not under the control of a single administrative entity, the fulfilment of fundamental network operations is heavily dependent on their cooperation. Nevertheless, individual interests in combination with resource constraints do not always encourage cooperative behaviour. In this work, we focus on static Wireless Mesh Networks (WMNs) and address the issue of selfishness in packet forwarding. Firstly, we model the dependencies that emerge in these networks as a result of their topology, traffic demand matrix, and route selection and determine the conditions for the natural emergence of collaboration, without the need of (monetary) incentives. We then assess the achievable collaboration levels, i.e., percentage of traffic demands (flows) that can be served thanks to the emerging collaboration, in both synthetic and real-world WMN topologies under shortest-path routing. Our results show that the cooperation improves when the number of flows increases. Yet, certain topological characteristics (marginal nodes, node degree distributions) make full cooperation difficult to achieve for the average case and bound it asymptotically. Finally, and motivated by these results, we use our dependency model to drive the selection of routes in the network. We cast the routing problem as a mixed-integer programming problem, which tries to maximize the collaboration level in the network. Our study finishes with an investigation of the resulting trade-off among network throughput, served traffic flows, and routing stretch factor. In the context of task 2.3, the paper examines WMNs' intrinsic resilience to selfishness, as well as a theoretical method for improving it. Based on the findings of this initial work, we are currently developing and implementing in the context of WP2 and WP4 a mechanism that will significantly reduce selfishness in mesh networks. The tasks outlined above can be integrated in the defense step of the ResumeNet strategy.

● 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

In this paper, we present a novel multipath structure called rope-ladder which combines the advantages of path, node and link protection schemes. It implements a defensive measure for our D^2R^2+DR resilience strategy which allows for delayed remediation. We also propose a position-based multipath routing protocol in order to efficiently construct rope-ladders in wireless networks. By design, the paths which are constructed by our protocol are closely together which allows to quickly switch back and forth between them in cases of node or link failures. Hence, the size of loss gaps (i.e., the number of consecutively lost packets) can be minimized. Previous works mostly confine themselves to overall packet loss comparisons. However, the loss gap size is crucial to ensure high quality for gap-sensitive traffic like voice flows. Our multipath structure can also tolerate failures of multiple consecutive nodes on the primary path, and has a superior path diversity and path lifetime compared to even perfect braids. We evaluate the performance of our protocol using analysis and simulations.

● 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

Because of our increased dependence on communication networks, resilience will need to be a fundamental property of the future Internet. We define resilience as the ability of a network to provide an acceptable level of service in light of various challenges, such as episodic connectivity or malicious actors. There have been many helpful point solutions to improve resilience in the Internet, but we argue a systematic approach is necessary to make resilience the first class citizen of the future Internet it needs to be. In this paper, we describe a general strategy for systematically embodying resilience in networks, called D^2R^2+DR. The strategy describes a real-time control loop to allow dynamic adaptation of a networked system in response to challenges, and an off-line loop that aims to improve the performance of

the network (the real-time loop) via a process of reflection. We demonstrate using an opportunistic networking scenario the application of the strategy, showing how it can be used to address the challenge of selfish nodes. We briefly describe our approach to quantifying resilience, and its use in our scenario. Finally, we show initial results from emulation that indicate that adapting forwarding behaviour in response to selfish nodes can improve message delivery in opportunistic networks.

● 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

At the core of the ResumeNet approach to resilience is policy-driven decision making. This is used to configure monitoring, detection and remediation/recovery mechanisms, for example. This paper explores the use of policies in the context of a specific scenario, demonstrating how they can be used to configure mechanisms that implement the D^2R^2 stages of the resilience strategy. It further justifies taking a policy-based approach to this, and demonstrates where research in the policy framework could be exploited to address some of the complexities of defining strategies for resilience.

● C. Doerr, and J. Martin-Hernandez, "A computational approach to multi-level analysis of network resilience", DEPEND 2010, Venice, Italy, July 18-25, 2010

This paper presents the computational side of the resilience quantification approach developed in Task 1.3. We demonstrate in a case study how this approach can be used to obtain hard performance guarantees and a detailed understanding of failure chains that will discover the root causes and subsequent effects of network challenges and, therefore, obtain deeper insights into the resilience of a network under stress.

● 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

P2P networks are one of the resilience mechanisms investigated in ResumeNet for providing resilient services. While application layer setup based on a P2P network may be a better solution than a server-based signaling solution in terms of reliability and survivability, it suffers from security and privacy issues since the data is stored and processed by some foreign peers in the P2P network which are not necessarily trustworthy. Taking VoIP as an example application, using a P2P network for the signaling requires users to store their current location (IP and port) in the P2P network. This information can be monitored by attackers and translated into a geographic location. This allows these attackers to build user location profiles. Moreover, during session establishment, foreign peers involved in the session establishment are able to notice that some users in the network have a social interaction with some other users. Since security and privacy are inherent to resilience, these issues need to be addressed adequately. In this paper, we present Pr2-P2PSIP, a Privacy-Preserving P2PSIP signaling protocol for VoIP and IM. Our contribution is primarily a feasibility study tackling the privacy issues inherent in P2PSIP. We leverage standard security protocols as well as concepts and experiences learned from other anonymization networks such as Tor and I2P where applicable. We present the design and on-going implementation of Pr2-P2PSIP and provide a threat analysis as well as an analysis of the overhead of adding privacy to P2PSIP networks. Particularly we analyze cryptographic overhead, signaling latency and reliability costs.

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

Critical to any defense and remediation strategy is a solid understanding of how a particular challenge spreads and affects a network. Recently, a number of social networking worms have spread over public Web sites. As immunization and error curing is frequently not fast enough, this paper investigates how

infections and challenges may be contained and limited in a network by temporarily disabling links, thus quarantining susceptible clusters in the network.

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

The work described in this paper fits in the WP4 of the project. Actually, in the experimentation part of ResumeNet, the aim is to exemplify our approach to resilience in concrete study cases, each one assessing a subset of the D^2R^2 + DR strategy aspects and the concepts/mechanisms realizing it. This study case is about service provision over heterogeneous smart environments. 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) has developed a mutualized technical platform allowing exchanges between applications across heterogeneous hardware and software. The 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. A platform, based on a messages publication/broadcast through subscription model (PubSub), realizes the filtering and routing functions of the middleware. This paper presents an approach for securing such a PubSub platform: availability and security (confidentiality, data integrity) are the targeted resilience criteria.

● E.K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J.P.G. Sterbenz, "A comprehensive framework to simulate network attacks and challenges", to be presented in 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. This paper makes a contribution to the work of WP2 in ResumeNet, as well as to the overall D^2R^2+DR framework of the project.

● T. Taleb, Y. Hadjadj-Aoul, and A. Benslimane, "Integrating security with QoS in Next Generation Networks", to be presented in 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. By integrating security with QoS, the devised approach ensures acceptable service resiliency, a key objective of the ResumeNet project.

● J.P.G. Sterbenz, E.K. Çetinkaya, M. Hameed, A. Jabbar, and J.P. Rohrer, "A framework for the analysis and simulation of network resilience", to be presented in the 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 analytical and simulation techniques for understanding, evaluating, and improving the resilience of the Future Internet.

2.4. Ongoing work

2.4.1. Papers under review

In addition to the publications listed above, there are 6 papers submitted covering work done in the project.

● W. Deng, M. Karaliopoulos, W. Mühlbauer, P. Zhu, X. Lu, and B. Plattner, "Using k-fault tolerance to characterize the resilience of Internet AS graph" – conditionally accepted to Elsevier Computer Networks (major revisions)

Various incidents in the past have revealed that the Internet is not as robust as it is widely thought. Evidently, there is the need to study the properties of the Internet in terms of resilience from a global perspective. We investigate in this paper the robustness of inter-domain communication, taking into account both topological connectivity and compliance to routing policies. To this end, we propose a method to efficiently determine whether a given Type-of-Relationship (ToR) graph corresponding to an instance of the Internet AS (autonomous system)-level topology is k-fault tolerant, i.e., reachability between any two nodes (ASs) can be maintained even after removing any arbitrary k nodes in the ToR graph. It turns out that the problem of determining whether a ToR graph is k-fault-tolerant is NP-hard. We apply our algorithm on large-scale data sets in order to study the resilience properties of the actual Internet. We find that a considerable number of additional AS-level edges (7; 747) will be needed to guarantee reachability even after arbitrary failures of one AS or AS-level edge in the Internet. Although any existing map of the AS graph is inherently incomplete, such numbers clearly point out that the robustness and resilience of the Internet as a whole is not as invulnerable as it is widely thought.

● A. Jabbar, H. Narra, and J.P.G. Sterbenz, "Quantifying resilience in mobile ad hoc networks" – submitted to IEEE INFOCOM, Shanghai, China, April 10-15, 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 to quantify multilevel resilience.

● A. Jabbar, and J.P.G. Sterbenz, "Towards quantifiable resilience for the future Internet" – submitted to ReArch, Philadelphia, PA, USA, November 30, 2010

While the Internet has shown itself to be robust on a global scale it is generally recognized that it is vulnerable to a number of challenges, such as attacks and large-scale disasters. One of the clear design goals for the future Internet should be to make the architecture fundamentally resilient. However, there

are no existing methodologies to quantify network resilience and the problem of evaluating resilience is known to be inherently complex. In this paper, we present a new framework that describes resilience in terms of two orthogonal dimensions: the operational state of a network entity and the state of the service that is expected from this entity. We illustrate the application of this framework with an example comparing the resilience of Internet topologies.

● G. Popa, F. Legendre, M. Karaliopoulos, and E. Gourdin, "Avoiding interference improves collaboration in multi-hop networks" – submitted to IEEE INFOCOM, Shanghai, China, April 10-15, 2011

In distributed network settings, where nodes are not under the control of a single administrative entity, the fulfilment of fundamental network operations is heavily dependent on their collaboration. Nevertheless, individual interests in combination with resource constraints do not always encourage collaborative behaviour. In this work, we focus on static Wireless Mesh Networks (WMNs) and address the issue of selfishness in packet forwarding. Firstly, we model the dependencies that emerge in these networks as a result of their topology, traffic demand matrix, and route selection and show that collaboration can emerge naturally, without the need for (monetary) incentives. We then assess the achievable collaboration levels, i.e., percentage of traffic demands (flows) that can be served thanks to the emerging collaboration, in both synthetic and real-world WMN topologies under shortest path routing. Our results show that the collaboration improves when the number of flows increases, which motivates our search for a collaboration-optimal routing method. Considering that only active nodes (sources or destinations) are members of the network, we examine the way an ideal interference-aware routing would impact the collaboration level. The main finding is that the type of route intersections generated by interference aware routing increases significantly collaboration among nodes that have full knowledge of the topology. To examine some of the properties of collaboration and to find conditions that support it, we use a number of mixed-integer programming models aiming at maximizing the collaboration level up to 100%. The results underline the fact that the optimal interference-aware routing also induces almost always optimal collaboration between the networked nodes.

● M. Schöller, P. Smith, and D. Hutchison, "Assessing risks for resilient networked systems" – submitted to Journal of Network and Computer Applications, Elsevier

Communication networks and the Internet, in particular, have become a critical infrastructure for daily life, business and governance. Ubiquitous connectivity is assumed everywhere and at all times. But most networks including the Internet have not been designed for this omnipresence. Various challenging conditions can render these networks or parts thereof unusable, with severe consequences. Building self-protection and self-healing mechanisms for all possible challenges is infeasible because of monetary, hardware and software constraints, and the impossibility to forecast all challenges associated with a network deployment. In this paper, we present a risk assessment process to identify the challenges with highest potential impact to a networked system and its users. The result of this process is a prioritised list of challenges, including associated system faults, which can guide network and system engineers towards the mechanisms that have to be built into the system in order to maximise resilience, while meeting the cost constraints. As we point out, this list is scenario dependent as the assets of the network users, the likelihood of a challenge occurring, and the probability of a challenge causing a service failure vary. A better understanding of these aspects and a way to determine reliable figures are open issues and open a new research space in the context of resilient and survivable networks.

● P. Van Mieghem, C. Doerr, H. Wang, J. Martin-Hernandez, D. Hutchison, M. Karaliopoulos, and R. Kooij, "A framework for computing topological network robustness" – submitted to IEEE/ACM Transactions on Networking

Currently, there does not seem to exist a commonly agreed definition of the robustness of a network, nor a framework to modify a network in order to meet some desired level of robustness. The goal of this article is to present a definition and a framework to *compute* topological network robustness.

2.4.2. Papers under submission

As the collaborative work in the consortium is a continuous process, the non-exhaustive list of joint publications in preparation includes:

● J. Lessmann, C. Doerr, J. Martin-Hernandez, and M. Schöller, "A highly-resilient challenge-aware protection scheme for multi-hop networks"

● M. Schöller et al., "Service isolation during remediation"

● P. Smith, M. Schöller, M. Karaliopoulos, C. Lac, D. Hutchison, J.P.G. Sterbenz, and B. Plattner, "ResumeNet: systemic network resilience"

3. Presentations

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

● 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

4. Publicity

In addition to the communication channels described earlier, ResumeNet has exploited other means (e.g., University magazines) to raise society awareness of its scope and objectives. "ETH Life", the magazine of ETH Zurich, has hosted an interview of Prof. B. Plattner, where ResumeNet is discussed in the context of the broader Future Internet topic.

● B. Plattner, "The future of the Internet", ETH Life, September 2009 (in German)

Download link: www.resumenet.eu/results/publicity

It is also worth mentioning a considerable collective effort of the consortium allocated to update and enhance the initial poster describing ResumeNet strategy and goals, as presented during the 2008 FIREWorks events. The improved version is available now on the Web site.

Finally, having participated to some events organized by the EC, e.g., The Future of the Internet (23-24 November 2009, Stockholm, Sweden), Future Internet Assembly Workshop (15-16 April 2010, Valencia, Spain), we have exploited the opportunity to deliver to the participants copies of this ResumeNet poster for publicity purposes.

Download link: www.resumenet.eu/project/brief

5. Further impact

Following on from the previous 'further impact' section, ResumeNet has continued to attract the interest of people and organisations, in Europe and beyond. Further links continue to be established with communities carrying out similar activities elsewhere in the world, notably through our highly active associate partners at the Universities of Kansas and Sydney.

The first case is, as before, in the USA through the work of J. Sterbenz at Kansas University, where ResumeNet has an ongoing connection with NSF GENI and related research activities. This continues to inform our work both in the scientific efforts on resilience (specifically in metrics) and in testbeds: we are again discussing the possibility of extending the GpENI testbed into Europe beyond the ResumeNet project. J. Sterbenz and D. Hutchison have been invited to a meeting between the EU and NSF in Brussels on 29 September, after the ICT 2010 conference, where this subject would be discussed. Also, D. Hutchison is exploring the same possibility with the Capacities part of the FP7 programme (Capacities funds, amongst other projects, the GEANT academic interconnect across Europe).

Second, D. Hutchison will be visiting Australia from late November through mid December 2010, and will spend time with Dr Peyam Pourbeik at DSTO, the Australian Defence Science and Technology Organisation (www.dsto.defence.gov.au) in Adelaide, who, as explained last year, is following the progress of ResumeNet. He will also spend time with M. Fry at the University of Sydney, who has been investigating joint activity within the context of Australian funding and who has also recently recruited a PhD student (namely Ms. Yue Yu) to work on ResumeNet. This student has been awarded a scholarship by NICTA, the Australian national ICT research institute (www.nicta.com.au): NICTA understand that this is an entry point to developing a relationship with ResumeNet.

Following the strong interest in the project by the delegation of the National University of Defense Technology (NUDT) of China and the subsequent work of PhD student Wenping Deng from NUDT as a guest at the Computer Engineering and Networks Laboratory of ETHZ from Nov 2008 to Nov 2009, an invitation has been issued by Lancaster University to Dr. Mixia Liu who has a Chinese Government scholarship following her work on Provable Security Design and Network Survivability Research, funded by the National Natural Science Foundation of China.

In the UK, BT Research has taken an interest in the work of the ResumeNet project, and is providing a new PhD studentship in the area of network resilience, to start in the autumn of 2010. Lancaster University will also fund a matching PhD studentship. These new resources will be associated with ResumeNet as well as with the work being done by Lancaster and BT within an India-UK research framework project on advanced networks research. This framework project, which is funded jointly by the Indian and UK Governments, links key Universities in the UK with the Indian Institutes of Technology. Through this route, the work of ResumeNet is becoming known within the Indian research community.

In Brussels, the work of ResumeNet has helped to inform the development of the 'FIRE Science' NoE call within FP7, and the related interest by the European Commission in Internet Science as a candidate theme for a FET Flagship: this follows from the Dagstuhl seminar that ResumeNet colleagues (G. Carle, D. Hutchison, B. Plattner, and J. Sterbenz) organized and ran in 2009 on the "Design of the Future Internet", in which key themes were identified, including resilience and security, as well as the need to involve other key disciplines in the debate around research agendas for the future of our network infrastructure.

Finally, ResumeNet has come to the attention of ENISA, the European Network and Information Security Agency, which works on behalf of the EU Institutions and Member States in response to security issues of the European Union. It describes itself as "the 'pacemaker' for Information Security in Europe" [ENISA]. We

have embarked on a dialogue with them about the resilience of networks, and ResumeNet will be represented at a forthcoming ENISA workshop on the subject of metrics to be held in Brussels later in 2010. Meanwhile, ResumeNet has completed a questionnaire prepared by ENISA on Measurement Frameworks and Metrics for Resilient Networks and Services. This is part of their Thematic Program which has the objective of collectively evaluating and improving the resiliency of public eCommunications in Europe.

6. Contribution to standardization work

The project Consortium has a good understanding of the challenges related to standardization and outlined very early its standardization strategy [DoW]; namely, that the impact of ResumeNet on standardization is primarily expected to happen *indirectly*, potentially via a Specific Support Action (SSA) and/or a Coordinated Action (CA) within FIRE. Nevertheless, the project has also invested resources on *direct* standardization actions. Such is the case with the ITU-T Focus Group on Future Networks.

Since its inception in 1865, the International Telecom Union has played a leading role in the most universally-recognized info communications standards, brokering industry consensus on the technologies and services that form the backbone of the world's largest, most interconnected man-made system [ITU_T]. In 2007 alone, its standardization sector (ITU-T) has produced over 160 new and revised standards (ITU-T Recommendations), covering everything from core network functionality and broadband to next-generation services like IPTV.

In the framework of ITU-T, Study Group 13 ("Future networks including mobile and NGN") leads the work on standards for next generation networks[1]. Convergence is a key word in this field. Built upon the Internet Protocol, the convergence between networks and/or technologies such as public switched telephone network, digital subscriber line, cable television, wireless local area network and mobile technologies is a task that many believe is impossible without the development of global standards [SG13].

SG13 has established in January 2009 a "Focus Group on Future Networks" to share the discussion on future networks and ensure global common understanding about these networks with collaboration and harmonization with relevant entities and activities [FG_FN]. By collaborating with worldwide future network (FN) communities (e.g., research institutes, forums, academia), this focus group aims to:

1. collect and identify visions of FN, based on new technologies,
2. assess the interactions between FN and new services,
3. familiarize ITU-T and standardization communities with emerging attributes of FN,
4. encourage collaboration between ITU-T and FN communities.

The inaugural meeting of FG-FN was held on 29 June - 3 July 2009 in Lulea (Sweden), i.e., the same week as the conference "*FIRE and Living Labs – Future Internet by the people*". ResumeNet, through a talk by M. Schöller entitled "*Network resilience as a prime feature of future networks*", has contributed to this collection and identification of future networks visions, by means of a presentation on resilience terminology and the ResumeNet strategy. The slides have been included as an official input document for the final report of the focus group to be published by the end of 2010.

Download link: www.resumenet.eu/results/standards

[1] NGN refers to the move from circuit switched to packet based networks that many operators worldwide will undertake in the next few years. It will mean reduced costs for service providers who will in turn be able to offer a richer variety of services.

References

[D5_2a] ResumeNet, "First Year Report on Dissemination Activities", Deliverable D5.2a, August 2009

[DoW] ResumeNet, "Description of work", 7th Framework Programme, Theme ICT-2007.1.6, New paradigms and experimental facilities, Grant agreement n° 224619, March 2008

[FG_FN] www.itu.int/ITU-T/focusgroups/fn/index.html

[ITU_T] www.itu.int/net/ITU-T/info/Default.aspx

[SG13] www.itu.int/net/ITU-T/info/sg13.aspx

[ENISA] ENISA work on resilience metrics, http://www.enisa.europa.eu/act/res/other-areas/metrics