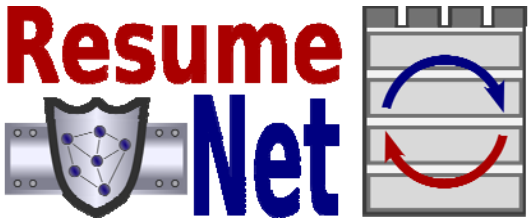
Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation



2nd ANNUAL PROJECT PERIODIC REPORT

(September 1st, 2009-August 31st, 2010)

Grant Agreement No.	224619
Project title	Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation
Deliverable number	D6.4d
Deliverable name	4th Periodic Progress Report
WP number	6
Delivery date	30 September 2010
Actual delivery date	29 October 2010, adjustment 11 November 2010
Editor	M. Karaliopoulos, R. Notz (ETHZ)
Contributors	A. Fessi (TUM), M. Karaliopoulos (ETHZ), C. Lac (FT), M. Schöller (NEC), P. Smith (ULANC)
Reviewer	B. Plattner (ETHZ)

Publishable summary

The research work carried out in the context of the ResumeNet project proposes a systematic architectural approach to Internet resilience that attempts to maximize interoperability with legacy network components.

In ResumeNet we understand resilience as the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to its normal operation. The term “service” includes the ability for users and applications to access information when needed (e.g., Web browsing and sensor monitoring), the maintenance of end-to-end communication association (e.g., tele- and video conferences), and the operation of distributed processing and networked storage. Our definition of resilience is therefore a superset of commonly used definitions for survivability, dependability, fault-tolerance, and performability. The challenges that may impact normal operation include unintentional hardware/software misconfigurations; large-scale natural disasters (e.g., hurricanes, earthquakes, ice storms, tsunami, floods); malicious attacks from intelligent adversaries against the network hardware, software, or protocol infrastructure, including DDoS (distributed denial of service) attacks; challenges related to the communication environment such as mobility, error-prone radio channels, and high latency; unusual but legitimate traffic load such as a flash crowds.

Our approach to understanding and implementing resilience in future networks evolves gradually within the project lifetime from the more abstract aspects of strategy and framework towards the more practical implementation issues.

At the highest level of abstraction the desired functionality of resilient networks is summarized in the six-step strategy D^2R^2+DR (Defend, Detect, Remediate, Recover, Diagnose and Refine). These straightforward Ds and Rs effectively order the required resilience functionality with respect to the nature of the different actions, i.e., proactive (preventive) vs. reactive, but also, more importantly, their timing: Detect, Remediate and Recover outline the shorter-term control loop in the operation of resilient networks, whereas Diagnose and Refine compose the outer, longer-term control loop. The six strategy components could be explained with the help of the metaphor of a mediaeval castle:

1. Defence, according to which the Internet is made robust to challenges and attacks (analogy: strong castle wall);
2. Detection of an adverse event or challenge that has impaired normal operation of the Internet and degraded services (analogy: guards on the castle wall);
3. Remediation in which action is autonomously taken to continue operations as much as possible and to mitigate the damage (analogy: boiling oil and fortification of internal walls when the castle wall is breached by a trebuchet);
4. Recovery to original normal operations once the adverse event has ended or the attacker has been repelled (analogy: cleaning up the oil and repairing the hole in the castle wall);
5. Diagnosis of the root cause of the challenge that impaired normal operation. This could be used to improve the system design and ease the recovery to a better state (analogy: determine the way in which enemy soldiers entered the inner walls of the castle); and
6. Refinement of future behaviour based on reflections of the previous cycle (analogy: construction of a thicker wall that will defend against current and predicted trebuchet technology).

A Framework for Architecture, Policies and Metrics

In engineering networked systems that are able to carry out these six operations, we need a good understanding of several concepts. Within ResumeNet this work is undertaken in the context of WP1 (framework) and involves a) understanding and characterizing challenges to the normal network operation and their impact; b) exploring proper metrics for measuring and assessing the network resilience; c) defining policies that can outline but also border the remediation space of the network; d) determining information sharing mechanisms within and among physical network entities for collecting, sharing, and correlating information from different protocol layers that will enable detection and remediation actions. The project work over the first two years of the project lifetime has covered all four main elements

We have developed a risk management based approach for assessing and classifying challenges to network operation. As starting point, our approach considers the critical assets associated with a system. Via step-by-step system analysis and identification of challenge scenarios, the approach builds an exposure graph that quantifies the risks related to the different challenges. The rationale is that the monetary and computational resources available for resilience are expected to be finite. Therefore, we need to understand the high impact challenges a networked system will face, so that defensive and remediation measures should primarily address those challenges.

On the metrics' side, Technical University Delft and Kansas University have been working on a multilevel framework that can assess the network resilience, as viewed by different layers of the protocol stack. Starting from the physical topology resilience, analysis and simulation are combined to get a view of how higher layers may attenuate or accentuate the impact of challenges on network performance, as this is experienced from different network functions and assessed from different viewpoints (e.g., user vs. network operator). A paper describing a framework for topological robustness has been submitted for publication to a highly prestigious journal. Our effort on mapping the topological resilience metrics to higher-level resilience metrics continues through the development of the Graph Explorer tool, a software tool that allows deriving bounds for the values of various resilience metrics by exhaustively searching over possible combinations of failures that may occur.

With respect to policies, we have investigated the features of three significant policy-based management frameworks – Ponder2, XACML and Or-BAC – that could be used for resilience. We found a number of useful features, which are described in the deliverable D1.3. Moreover, in a publication submitted to AIMS 2010, we described the application of policies to a resilience case study: high traffic volume challenges to an ISP's infrastructure.

Finally, our work on understanding the various approaches to information sensing and sharing continues, with a strong cross-layer dimension embedded to it. Joint work between Kansas Univ. and Lancaster Univ. on exploring the trade-offs associated with performing error control in different ways, given distinct application requirements, has continued with the implementation of a number of error control mechanisms for the ns-3 simulator at the hop-by-hop and end-to-end levels. Initial simulation results, along with a cross-layer formalism, which form the beginnings of a cross-layer framework, are described in D1.4. In addition, D1.4 describes a set of requirements for information sources to aid decision making for resilience, e.g., when detecting and remediating challenges. This study includes a critical survey of cross-layering techniques and monitoring systems. Also, it explores the use of context information to better understand the nature of a challenge. The utility of the various information sources discussed is shown in a number of case studies.

The work on framework then inputs to the studies of mechanisms in WP2 and WP3.

Making the Network More Resilient

First, we explore and develop a set of architectural principles on which resilient systems in general, and the Internet in particular, should be based. Examples of such principles are self-protection,

redundancy, diversity, with their corresponding resource tradeoffs. We consider how these could be realized at different network levels and functions, e.g., at topology level, in routing, or as part of transport protocols; but also at the application level via use of peer-to-peer and overlay routing or virtualization. Research effort is also put on particular processes that can be viewed as the building blocks of resilient networking such as monitoring, learning processes, and decision engines. It is, in fact, the synthesis of these blocks that will enforce resilience to the various network layers. One of the questions pursued in the project is to what extent could their systematic definitions ease their reuse and result in scalable solutions.

More specifically, in WP2, work is organized around the 2 Ds (Defense, Detect) and one R (Remediation) of the D^2R^2+DR strategy.

More specifically, ResumeNet is pursuing five different defensive measures on different layers of the protocol stack. The first approach is looking at “topological conditions for collaboration in wireless mesh network”. The goal is to provide defensive measures to the network layer to protect the distributed system from maliciously behaving nodes, i.e., forwarding selfishness. A protocol leveraging these results is currently under development as a WP4 work item. The second approach focuses on “optimization models for resilient network design”. The developed optimization model outputs a network topology which balances resilience and monetary costs. “Diversity in topology and end-to-end mechanisms” is the third measure under investigation. It has three main thrusts: firstly, the identification and characterization of multiple reliability modes; secondly, Path Diversification, a heuristic approach to selecting multiple end-to-end paths for simultaneous or failover use, and third the modelling of physical topologies, network attacks and challenges. Verification of the simulation models on the GpENI infrastructure is planned. The fourth approach is looking at integrating QoS with Quality of Security (QoS^2). This defensive measure balances quality of service versus quality of security using a multi-attribute decision making algorithm. The algorithm was evaluated for an IPTV service environment. The fifth defensive measure investigates the required protection each node has to provide to protect the overall system from malware. This activity is called “Protection against malicious information spread”. A model of the spreading process has been developed and applied with different configurations.

With respect to challenge detection, an extensive literature study and consolidation effort had to be performed first since this has been a research topic for several years. Based on these results, ResumeNet partners have been pursuing four different research threads. The first thread addresses challenge detection in wireless mesh networks, focusing on interference. The second research area is about challenge detection in opportunistic networks, where the detection task is severely hindered by episodic connectivity. The third research item evolves around an information storage and sharing architecture to support challenge detection and fault analysis. The last research item, closely related to the third one, draws on the proposed information storage mechanisms to autonomously self-refine the challenge detection architecture.

The last task in WP2 is concerned with the adaptation that is necessary to remediate the network once challenges are detected. A second step will investigate system evolution and refinement of the resilience architecture in year three of the project. ResumeNet partners have investigated three different scenarios to extract requirements for such a system adaptation: a wireless mesh backhaul network, an opportunistic network, and an enterprise service network. Based on these requirements an architecture for network resilience has been derived. Further investigations have been focusing on technologies for this resilience architecture: remediation strategies using adaptation of access control policies, remediation strategies using obligation policies to adapt the system configuration and specialized optimizers supporting the remediation selection process. An example how a specialized optimizer, i.e., the graph explorer tool, can be used to construct and advise the repair of our rope-ladder multi-path structure has been started. Furthermore, research on containing remedies in isolated virtual networks is generating the first results.

Towards Resilient Services

WP3, launched in parallel with WP2, investigates different resilience mechanisms which are complementary to WP2. The focus in this WP is on service resilience. The general approach is to use techniques which can provide abstractions from the underlying hardware resources and thus can proactively (Defence) improve the resilience of services. These techniques are, more specifically: a) P2P; b) overlay-based end to end connectivity; and c) virtualisation.

P2P signalling is used to provide resilient lookup of a communication partner (IP and port), e.g., for VoIP call, or a web session. Protocols used for this purpose today are, e.g., DNS or SIP while the actual data is transported subsequently using, e.g., HTTP or RTP. For the SIP case, we follow a supervised P2P approach with endpoints as peers and a central authority as a server. We have provided a quantitative reliability model based on reliability theory and traces from the Skype network. For the DNS case, we have evaluated the suitability of P2P networks for resolving DNS Fully Qualified Domain Names (FQDN) and came across hot spot problems. However, we are currently learning from DNS deployment, notably the usage of IP anycast for reaching DNS servers, and want to apply IP anycast as a resilience mechanism to maximize service availability over the network.

The next resilience mechanism in WP3 is overlay-based end-to-end connectivity. At the data plane (e.g., HTTP or RTP) if the end-to-end communication using TCP/IP between the two endpoints is disrupted, then overlay-based end-to-end connectivity comes into place. A P2P overlay network is used for providing end-to-end connectivity as a failover. Additionally, services can be hosted in virtualised environments. Hosting services in virtualised platforms is a Defence itself, (since it provides isolation and thus better security), but is also an enabler for the migration of services as a Remediation and Recovery strategy. In this context, the costs and implications of different migration techniques are currently being investigated.

While work in WP3 has a strong focus on defence, i.e., proactive resilience mechanisms put in place before challenges occur, the remaining three steps of the inner loop (Detect, Remediate and Recocer) at the service level are among the contributions of France Télécom in the project.

This task is integrated with the overall challenge identification architecture in WP2. It reuses results from WP1, notably the work on policies, to select and apply remediation mechanisms. And finally, the results of this task flow into the experimentation activities in WP4.

Experimental Validation

The evaluation of both principles and mechanisms is carried in WP4 out via analysis and experimentation. Four case studies have been defined to exemplify the application of the framework in concrete service provision scenarios. They represent a well-balanced mix of networking paradigms with both short-term and longer-term potential for commercial exploitation such as Wireless Mesh Networks, Delay Tolerant Networks, and Internet of Things. Experiments are carried out on testbeds; some of them are in-house experimentation facilities, deployed or enhanced for the needs of the project (e.g., ETH Zurich TikNet, Uppsala Haggle testbed), whereas others are larger-scale facilities made available to the research community via dedicated projects (e.g., Planetlab and its European counterpart, Planetlab Europe).

During the first two years of the project, significant effort has been devoted to the more detailed specification of the experimentation scenarios and the respective testbed development work, where appropriate. This work is directly influenced by the progress made on the framework (WP1) and mechanism (WP2-WP3) aspects of the project. In parallel, the activities in WP4 have supported the activities of the EU FIREWorks Coordination Action[1] via compilation of two versions of two light deliverables on the federation requirements and the links between research and experimentation in ResumeNet.

[1] http://www.ict-fireworks.eu/

Impact

Overall, ResumeNet aims at having a broader socio-economic impact by contributing, though not to the same extent, to the following four points, as quoted from the FP7 ICT Work program for 2007-08 for the strategic objective ICT-2007.1.6:

- Strengthened European position in the development of the Future Internet.
- Wider take-up of technological developments in networks and service infrastructure facilitated by a comprehensive validation of the technological and service choices.
- Global consensus towards standards and strengthened international cooperation through interconnected test beds and interconnection capabilities offered to third countries.
- Higher confidence in the secure use of the Internet through enabling trusted access to e-Services.

With this in mind, ResumeNet has devoted considerable effort in the first two years to the dissemination of its results:

1. The project Web site and Wiki pages are operational since November 2008 (http://www.resumenet.eu/). The public website pages have seen one major update during August 2009, which involved both information and presentation aspects, and are regularly updated with the latest project news and results.
2. ResumeNet has been presented, with the use of flyers, posters2, or slide sets, in various venues including magazines; scientific conferences and workshops; events organized by the European Commission (SAC/FIRE Workshops, FIRE Launch Event, ICT 2008-2010). In the same time, significant work carried out within the project has been published in conferences and scientific journals. Last, but not least, local media have hosted interviews of ResumeNet Consortium members on the relevance of ResumeNet work to the future Internet.
3. ResumeNet has been closely monitoring the activities of the Future Internet Assembly, supporting the coordination activities of FIREWorks, and participating in the meetings of the FIRE Expert Group. The project has also invested resources on direct standardization actions. Such is the case with the ITU-T Focus Group on "Future Networks", established in January 2009 by Study Group 13 ("Future networks including mobile and NGN").
4. A Dagstuhl Seminar on "Architecture and Design of the Future Internet" was organized by G. Carle, D. Hutchison, B. Plattner, and J.P.G. Sterbenz, all partners of the ResumeNet project, on 14-17 April 2009. Prominent researchers and practitioners with interests in the area of networking were invited to exchange views on trends and proposals about the future of communication networks.
5. Members of the project published five papers in prestigious journals, two magazine articles and 23 articles in peer reviewd conferences or workshops. Six more articles were submitted for publication.
6. ResumeNet also has an impact on education in the involved academic institutions, with six Bachelor theses and eleven Master theses on-going or completed. Fourteen Doctoral theses are on-going and two were completed in 2010.

Exchanges have also taken place with EU projects carrying out activities on network resilience. Contacts have been made to the FP6 Network of Excellence ReSIST (http://www.resist-noe.org/) to ensure that ResumeNet actors and results will be included in the Resilience Knowledge Base, one of the main deliverables of ReSIST. Chidung Lac (FT), the leader of ResumeNet WP5, is part

[2] The latest version of ResumeNet's poster is available now in the public Web site.

of the Advisory Board of the FP7 Coordination Action AMBER (http://amber.dei.uc.pt/), which focuses on resilience measuring, assessment and benchmarking. Similar interactions have been possible during the first project year with the FP6 Integrated Projects ANA (Autonomic Network Architecture) and Haggle, as well as with the FP7 project ECODE, thanks to common partners in those Consortia.

Further evidence to the impact ResumeNet has had so far comes from companies and institutions that approached the project and expressed their intention to initiate their own research activities on the topic of network resilience (Australian Defence Science, Technology Organisation, National University of Defense Technology (NUDT) of China, Telecom Malaysia) or link existing ones to the ResumeNet work (OFCOM, QinetiQ and BT in UK).

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. The project members 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 resilience metrics to be held in Brussels later in 2010.

http://www.resumenet.eu

Contact details:

Prof. Dr. Bernhard Plattner

Project Coordinator

ETH Zurich

Computer Engineering and Networks Laboratory

Address: Gloriastrasse 35

CH-8092 Zurich

Switzerland Telephone: +41 44 632 7000

Fax: +41 44 632 1035

Contents

1. Project objectives for the 2nd year of the project

The project activities during this second year of the project were focussed on three main objectives:

Making progress in the research work on network resilience framework and mechanisms: The major research efforts in the project were to be in the context of WPs 1-3.

Key framework ingredients, particularly metrics and policies, had to be further pursued and developed to be able to steer work within WPs 2 and 3. Deliverables D1.2a, D1.3a, and 1.4a have addressed the individual framework components (policies, metrics, and information sharing mechanisms), while D1.5b provides the overall framework and describes how the pieces fit together in the whole puzzle.

Moreover, considerable work, according to the time schedule, had been planned for WP2 and WP3, the emphasis being more on the short-term, real-time control loop that consists of the Defend, Detect and Remediate components. In WP2. a series of deliverables was planned in DoW for each of the three components: D2.1a and D2.1b for defensive measures, D2.2a and D2.2b for the challenge detection part, and D2.3a and D2.3b for the Remediation part. Likewise, the work in WP3 would deepen on architectural aspects (D3.1b and D3.2) and would initiate the study of more specific mechanisms such as P2P and virtualization (in D3.3).

Initiating the experimentation work: The experimentation work of the project was scheduled from the beginning for the second half of the project. During the first six months, the finalization of the scenarios and the initial developments of software modules were to happen together with some initial experimentation via simulation and/or testbeds and be reported in D4.2a.

Strengthening the integration of partners' effort in the project: This third objective stood in close relation to the first two purely research-oriented objectives. A higher integration of efforts was also requested by the reviewers of the project during the 1st review meeting. This integration can be achieved using two distinct approaches. First, it can be done by having the appropriate partners more actively cooperating in the context of the project tasks. This can happen at different intensities and can be realised in different ways ranging from the joint preparation of a paper or technical report to the exchange and integration of software. Second, integration is, in principle, feasible at the experimentation phase of the project. Again, the intensity may vary: it may happen through experimenting with various aspects of the research work, carried out by different partners; or, it may involve putting together piece of hardware of software, developed by different partners, in a single integrated experiment. Given that the experimentation activities of the project officially started at M18, the main effort would be in this 2nd year to foster more integration with the first approach. In parallel, there would be further discussions and iteration on regarding the experimentation strategy.

These three objectives are in-line with the recommendations made by the reviewers during the 1st project review meeting. Although they did not call for any significant change of project objectives, they called for higher "integration" of efforts. In summary, their man request were:

> 1. Further integration of the consortium effort that could leverage the variety of skills and knowledge in the project Consortium. In some cases, this would mean the merging or combined investigation of topics, especially modelling efforts, which have been explored in isolation so far. With respect to experimentation this would mean, if

possible, integrated experiments combining modelled failures and resilience mechanisms in multiple locations and at multiple layers.

2. Better linking of the research work to the overall framework concepts and promotion of the cross-layer and distributed nature of resilience.

With respect to dissemination, the aim was set to disseminate these first project results in places (conferences and workshops), where prompt feedback could be obtained. In parallel, it had been discussed within the Project Consortium that effort should be devoted to strengthening links with real players in the networking arena (e.g., network operators, service providers). This would let the project research be shaped by their requirements and have an impact on them.

In the following sections, we summarize the steps made along these directions during year 2 of the project.

2. Work progress and achievements during the period

2.1. WP1: Framework for resilience and networking

2.1.1. Per-task summary of progress towards objectives

Task 1.1 Strategy for resilient networking

Our ongoing work on consolidating the activities in the project have, amongst other findings, led us to develop a new diagrammatical representation of the D^2R^2+DR strategy, which was used as part of a paper that is to be submitted to IEEE Communications Magazine. This proposed paper, along with a published article that formed an introduction to an Elsevier Computer Networks special issue on resilient network, constitute the main contribution of D1.5b, the second interim strategy document for resilient networking. The diagram reflects our current understanding of the resilience problem, in that the real-time loop is more understood than the outer loop, which is to be investigated in the final year of the project.

Task 1.2 Understanding Challenges

This activity officially finished in M6 of the project. However, during this reporting period we have further developed the risk assessment process described in D1.1 and submitted an article to a special issue of the Elsevier Journal of Network and Computer Applications.

Task 1.3 Resilience metrics

Our effort on multi-level resilience metrics continues through the development of the Graph Explorer tool. Our findings on this have been published in the third international conference on dependability (DEPEND 2010). The Graph Explorer tool is also being used as part of an investigation in WP2 that uses its output to inform better (rope ladder) multi-path forwarding structures. Furthermore, the exploration regarding multi-level metrics is being investigated in a framework to quantify network resilience, which is described in a PhD thesis, which was completed during this reporting period.

Task 1.5 Cross-layer optimisation and multi-level resilience

Our work in this task on understanding the various approaches to cross-layering continues. Joint work between Kansas Uni. and Lancaster Uni. on exploring the trade-offs associated with performing error control in different ways, given distinct application requirements, has continued with the implementation of a number of error control mechanisms for the ns-3 simulator at the hop-by-hop and end-to-end levels. Initial simulation results, along with a cross-layer formalism, which form the beginnings of a cross-layer framework, are described in D1.4. In addition, D1.4 describes a set of requirements for information sources to aid decision making for resilience, e.g., when detecting and remediating challenges. This study includes a critical survey of cross-layering techniques and monitoring systems. Also, it explores the use of context information to better understand the nature of a challenge. The utility of the various information sources discussed is shown in a number of case studies.

2.1.2. WP1 Main Output

The following summarises the main results from WP1 for this reporting period:

- Delivery of the interim deliverable D1.5b on a “strategy document for resilient networking” and D1.4 on a “Cross-layer optimization and multilevel resilience”.
- Implementation of error control mechanisms for the ns-3 simulator as part of ongoing work on understanding cross-layer trade-offs.

·Submitted an article for review to a special issue of the Elsevier Journal of Networks and Computer Applications, entitled “Assessing Risk for Resilient Networked Systems”.

The following publications:

1. C. Doerr, and J. Martin-Hernandez, “A computational approach to multi-level analysis of network resilience”, DEPEND 2010, Venice, Italy, July 18-25, 2010
2. Abdul Jabbar, "A framework to quantify network resilience and survivability", PhD thesis, May 28th 2010

2.1.3. Deviation in the time plan and the WP structure from the technical annex

None

2.2. WP2: Network-level resilience

2.2.1. Per-task summary of progress towards objectives

Task 2.1: Defensive Measures

This task researches defensive techniques and mechanisms to resist challenges, so that the network is likely to remain operational even when challenged or attacked. ResumeNet is pursuing five different measures on different layers of the protocol stack. The first approach is looking at “topological conditions for collaboration in wireless mesh network”. The goal is to provide defensive measures to the network layer to protect the distributed system from maliciously behaving nodes, i.e., forwarding selfishness. A protocol leveraging these results is currently under development as a WP4 work item. The second approach focuses on “optimization models for resilient network design”. The developed optimization model outputs a network topology which balances resilience and monetary costs. “Diversity in topology and end-to-end mechanisms” is the third measure under investigation. It has three main thrusts, first the identification and characterization of multiple reliability modes, second Path Diversification, a heuristic approach to selecting multiple end-to-end paths for simultaneous or failover use, and third the modelling of physical topologies, network attacks and challenges. Verification of the simulation models on the GpENI infrastructure is planned. The fourth approach is looking at “QoS2: Integrating QoS with Quality of Security”. This defensive measure balances quality of service versus quality of security using a multi-attribute decision making algorithm. The algorithm was evaluated for an IPTV service environment. The fifth defensive measure investigates the required protection each node has to provide to protect the overall system from malware. This activity is called “Protection against malicious information spread”. A model of the spreading process has been developed and applied with different configurations.

The results of this task are presented in Deliverable D2.1b submitted as a M24 deliverable.

Task 2.2: Challenge Detection

This task is concerned with the detection of challenges that threaten normal operation and that have breached the defensive measures. Challenge detection is a research topic for several years. Therefore, an extensive literature study and consolidation effort had to be performed first. Based on these results, ResumeNet partners pursued four different research objectives. The first objective focuses on “challenge detection in wireless mesh networks”, especially the detection of signal interference. The second objective is targeted at “challenge detection in opportunistic networks”. Due to the episodic connectivity special problems for challenge detection arise. The third objective is to pursue research for an information storage and sharing architecture to support challenge detection and fault analysis. The fourth objective targets an autonomously self-refining network measurement challenge identification architecture based on the proposed information storage.

The results of this task are presented in Deliverable D2.2b submitted as a M24 deliverable. Both activities are expected to continue in the third year of the project to finalize this work

Task 2.3: Adaptation and Evolution Framework

This task is concerned with the adaptation that is necessary to remediate the network once challenges are detected. A second step will investigate system evolution and refinement of the resilience architecture in year three of the project. ResumeNet partner’s investigated three different scenarios to extract requirements for such a system adaptation: a wireless mesh backhaul network, an opportunistic network, and an enterprise service network. Based on these requirements an architecture for network resilience was derived. Further

investigations focused on technologies for this resilience architecture: remediation strategies using adaptation of access control policies, remediation strategies using obligation policies to adapt the system configuration and specialized optimizers supporting the remediation selection process. An example how a specialized optimizer, i.e., the graph explorer developed in T2.1, can be used to construct and advise the repair of our rope-ladder multi-path structure has been started. Furthermore, research on containing remedies in isolated virtual networks is showing first results.

The results of this task are presented in Deliverable D2.3b submitted as a M24 deliverable.

2.2.2. WP2 milestone

- M2.1 First demonstrator of the optimization tool for resilient network topologies
- M2.2 First prototypes of the Adaptation and Evolution Framework

The two software milestones have been reached in M22 and M24 respectively. Therefore, the partners have made their software contributions available on the project svn server for other partners to use them for further work. This has lead to collaborative activities such as the ongoing work of integrating the rope ladder routing scheme (developed by NEC) with the graph explorer (developed by TUDelft) as one particular example.

2.2.3. WP2 main output

The following summarises the main results from WP2 for this reporting period:

3. Delivery of three interim deliverables: D2.1a on defensive measures, D2.2a on challenge detection, and D2.3a on the resilience framework.
4. Delivery of three final deliverables: D2.1b on defensive measures, D2.2b on challenge detection, and D2.3b on the resilience framework.
5. Fulfilling the WP2 milestones M2.1 and M2.2
6. 18 papers published from T2.1 work on defensive measures
7. Three papers published from T2.2 on challenge detection
8. Eight papers published from T2.3 on the adaptation framework
9. At least three additional publications from WP2 partners are currently under preparation

2.2.4. Deviation in the time plan and the WP structure from the technical annex

According to the description of work, tasks 2.1 and 2.2 had to conclude their respective research in M24. The results of these tasks have revealed that there are still open interesting research questions which ResumeNet partners have not been able to address yet.

For example the usage of XTrace in the challenge detection phase opens new possibilities for network internal measurements which promises better challenge identification approaches. Thus an extension of the tasks duration and a reassignment of resources from other tasks have been requested from EC.

2.3. WP3: Service-level resilience

2.3.1. Per-task summary of progress towards objectives

Task 3.1: Resilient services framework

Task 3.1 is an umbrella task for WP3 and is an on-going task during the whole WP3 period. It has been coordinating the activities with other WPs as well as within WP3, in particular integration activities, e.g., between resilient P2P signalling and virtualisation. One result of this task is D3.1b (delivered in April 2010) which describes the ResumeNet interim resilient service architecture, notably how the components i) P2P signalling, ii) virtualisation, iii) challenge detection and iv) overlay-based connectivity interact with each other.

Task 3.2: Secure application of P2P and overlay networks for resilient service provision

Work on Task 3.2 carried by TU Munich focuses on how P2P networks can be used for building resilient services. As mentioned in previous progress reports, two types of architectures or protocols have been considered: i) SIP and ii) DNS.

In the SIP case, we have been investigating the application of resilient SIP signalling on top of a P2P network with the goal to establish application sessions, e.g., VoIP. We provided a solution for supervised P2P signalling called Cooperative SIP (CoSIP) described in D3.3 (delivered in August 2010). We provided a quantitative reliability analysis based on reliability theory and traces from the Skype network. An extensive threat analysis in D3.3 describes to what extent a supervised approach can address the security threats inherent in P2P networks and what additional security mechanisms are required.

Some of the security threats which arise from the deployment of a P2P network for SIP signalling are attacks on user location privacy and social interaction privacy. A solution to address these privacy issues was developed and published at ACM IPTComm 2010.

As for the DNS case, while our approach for a P2P DNS system differs from earlier approaches in this direction in several aspects, extensive simulations have shown that it is very hard issue to provide a competitive solution based on P2P networks. The main issue is the power-law distribution of the popularity of DNS Fully Qualified Domain Names (FQDN). This skewed popularity distribution would lead to extreme hot spots in the network. These hot spots are currently absorbed by the operators of the DNS root servers and the Top Level Domain (TLD) Servers but can not be tolerated by the end hosts in a P2P environments. However, we have learned interesting aspects of the DNS operation, notably the root and TLD servers. IP anycast has been deployed to achieve failover between DNS server nodes reachable under the same IP address but located in different geographic locations. We are currently in the process of analysing the generic applicability of IP anycast for resilient services. For this purpose, we use traces collected at the anycast DNS A-root server in February this year.

Task 3.3: Management and security of virtualization services

As mentioned in previous progress reports, this task investigates the application of virtualization mechanisms to achieve service resilience. In particular, the migration of virtual services is used as a resilience enabler. Services can be encapsulated in virtual machines, thereby abstracting from the underlying physical hardware. Upon encountering challenges in the form of hardware shortcomings, the virtualized services can then be migrated from one physical machine to another.

In order to classify migration mechanisms that can be used for these goals, the phases of virtual service migration have been identified. Using virtualization as a resilience-enabler depends on the challenge detection mechanisms developed in WP2 and WP3. Once a challenge has been identified, the current state of the virtualized service has to be migrated.

After the migration, network traffic has to be redirected in order to allow service clients to find the virtualized service at its new location. Finally, once the challenge is over, the virtualized service has to be migrated back to its original location. These different phases were elaborated in deliverable D3.1b (delivered in April 2010).

Since different migration mechanisms provide different advantages and disadvantages, a resilience-aware management of migration mechanisms is needed. An architecture for resilience-aware migration management has been proposed in deliverable D3.3 (delivered in August 2010).

Task 3.4: Service surveillance and detection of challenging situations

As explained in D6.4c, this task is about the Detection/Remediation/Recovery (DR^2) phases of ResumeNet's D^2R^2+DR strategy. It aims at building a framework for monitoring any service requiring a certain level of resilience. To this end, probes need to be inserted at the proper location in order to detect abnormal events. Their outputs, called `alarms', are analyzed and treated using a correlation engine which requires as input a clear definition of challenging situations, including the resilience metrics used, for the service under study. The outcome of this analysis, i.e., a challenge detection called `alert', will trigger remediation, e.g., with the help of policies deployment/modification. Continuous monitoring and event analysis provide information about the end of the threat, leading to actions to recover the system, bringing the service back to its normal performance operation.

Challenge detection, also realized in ResumeNet but at a network level (Task 2.2), led to a general architecture adopted in the project for this DR^2 purpose; together with the Publish/Subscribe distributed store for challenges and remediation, it constitutes the framework we use as well. The work done during this reporting period, and detailed in D3.2 (delivered on July 2010), can be summarized as follows:

- Survey of basic monitoring principles, focusing on general policy, techniques, data, and maintenance operations.
- Presentation of events correlation, i.e., fault localization.
- Description of chronicles recognition, the correlation engine we shall use for challenge detection.
- Illustration of this technique through some applications of it in networks and services alarms analysis for security-related objectives (intrusion detection, reflexive DDoS attack), or dependability-related concerns (recovery actions monitoring, handover initiation in mobile systems).
- Use of a dynamic policy engine for the Remediation phase, i.e., reaction to an alert generated by the correlation analysis, through the experimentation scenario "Communicating objects' data platform" which will be deployed as a service use case in Task 4.4.

Task 3.5: Overlay-based end-to-end connectivity

As mentioned in previous progress reports, this task aims at providing end-to-end connectivity using an overlay as a failover technique. It is intended for cases where IP connectivity is disrupted in a way such as a host can only reach parts of the Internet, e.g. due to major BGP convergence problems. Previous work in this area suffered from scalability problems. The overlay would be limited to about hundred nodes. Thus, in Task 3.5 we are in the process of developing a scalable routing protocol that allows for more nodes by orders of magnitude. The key idea is to store the relevant information about connectivity in a DHT, which then can be accessed by the actual routing protocol to establish new forwarding paths

on-demand. To accelerate the establishment of required new routing paths, the data need to be pre-processed in a way such as the gathering of the required information to establish a path can be found efficiently. A requirements analysis and interim architectural draft for Task 3.5 can be found in the appendix of D3.1b. An evaluation framework is being investigated and will be documented in D3.4 (Feb. 2011).

2.3.2. Deviations from the time plan and suggestions for correction

Mihail Andries, one of D6.3's contributors, has resigned from FT at the end of September 2009. Until August 2010, there has been no replacement. For this reason, the work in Task 3.4 is delayed. As a consequence, D3.2 (Service Surveillance), due in June 2010 (M22), is an interim version. The final version of the results of T3.4 will be described in D3.1c (Resilient Service Architecture - Final) which is due in August 2011 (M36).

2.3.3. WP3 main output

The following summarises the main results from WP3 for this reporting period:

- D3.1b with the interim resilient service architecture.
- D3.2 with a framework for challenge detection in line with the challenge detection activities in WP2.
- Quantitative reliability models of P2P networks and their application for VoIP signaling (see D3.3).
- Mechanisms to address P2P security issues and make them suitable for building resilient services (see D3.3)
- Investigated privacy issues raised by resilient P2P VoIP solutions, and published a paper at ACM IPTComm 2010.
- Evaluation of P2P alternatives for DNS through simulations and understanding the risks.
- Early investigations of the impact of IP anycast on DNS resilience.
- Evaluation of the implication of migration of services running in virtual machines and a publication in preparation to be submitted to KIVS 2011.
- Performed state-of-the-art analysis and laid out architecture for overlay-based end-to-end connectivity (Task 3.5 is on-going until Feb. 2011).

2.4. WP4: Experimental Evaluation of resilient networking

In the experimentation part of the project, the aim is to exemplify our approach to resilience in concrete study cases. Work Package 4 (WP4) has been structured around study cases, which are effectively combination of {networking technology, service provision scenario, challenge set} tuples. The four scenarios are:

1. Forwarding Selfishness in Wireless Mesh Networks (w)
2. Content Dissemination in Opportunistic Networking (o)
3. Cooperative Session Initiation Protocol (s)
4. Publish-Subscribe Platform for Smart Environments (p)

Each one assesses a subset of the D^2R^2+DR strategy aspects and the concepts/mechanisms realizing it (ref. Table 1 in D4.2a).

The main effort so far has been devoted to the more detailed specification of the experimentation scenarios and the respective testbed development work, where appropriate. This work is directly influenced by the progress made on the framework (WP1) and mechanism (WP2-WP3) aspects of the project.

The related activities are summarized in the deliverable D4.2a, submitted to EC in M24; earlier status summaries exist in deliverables D4.1b and D6.2b, which have been submitted to FIREworks in M18.

2.4.1. Per-task summary of progress towards objectives

Task 4.1. Resilient routing and medium sharing in Wireless Mesh Networks

Monitoring and management software has been developed for the Wireless Mesh Network testbed, which is deployed at the G floor of the Department of Electrical Engineering and Information Technology, in ETH Zurich. In addition to this, the basic software and hardware of the testbed have been upgraded to more recent versions.

Current development effort is related to the assessment of the cooperation-friendly routing protocol developed by ETH Zurich and consists in:

- Developing a software module residing on every station whose purpose is to compute based on traffic requirements and power level when to apply a selfish strategy and when not. Note that the number of selfish nodes should remain fairly low as long as the throughput requirements from other stations remain also low.
- Construction a theoretical method based on network coding with the goal of improving throughput and eliminating selfishness. The method is based on the fact that the incentives of relay nodes will force them to exchange coded packets (which contain a linear combination of both useful and not useful packets for that relay) with other stations.
- A software module running on each individual machine (source node) which responds to changes in the level of cooperation, by applying the aforementioned network coding-based strategy.

Task 4.2. Resilient forwarding in opportunistic networks

Our experimentation is two-fold. We investigate the impact of node misbehaviours on opportunistic networks and aspects related to congestion management. Experimentation is performed on the in- house Haggle testbed that runs on both mobile phone and virtual machines, as well the ONE emulation framework from Helsinki University. The testbed allows

emulating a mobile opportunistic network and conducting repeatable tests in a controlled and easy to manage environment.

During the reporting period we worked on the following issues:

- Improved stability and adjusted the Haggle testbed for experimentation and implemented a full control loop of the ResumeNet strategy. The work got published at the Mobile and Future Internet Summit.
- In an approach to challenge detection, we evaluate verifiable service agreements where nodes promise to carry messages for a certain time interval. We investigated the effect of data aging on data delivery and delay for different time intervals and plan as a next step to formulate an algorithm to chose a time interval given characteristics of the scenarios.
- Congestion control was in our focus in general. We investigated methods to manage buffers and choosing data to be forwarded. So far we run experiments to better understand the relations between the parameters and data delivery and delay.
- First selfishness and attack scenarios have been identified together with ETHZ and initial experimentation with the ONE simulator has begun.

Task 4.3. Service-level resilience evaluation

TUM has been conducting its testbed activities in WP4 inline with the work in WP3. The implementation of cooperative SIP signalling between DHTs and servers (CoSIP) was ported from the Bamboo DHT implementation[3], which is in Java to a Kademlia implementation in Python called Entangled[4], not only because the CoSIP engine was implemented in Python, but also because Kademlia has interesting properties from resilience point of view. Furthermore, tools have been developed to setup a highly distributed CoSIP testbed with 400-500 peers on PlanetLab (currently only one CoSIP peer per PlanetLab node is possible). The peers emulate phone calls regularly. The CoSIP implementation was enhanced by diagnostic tools. Diagnostic data are sent regularly to a server at TUM for further evaluation. Currently, a web site is under construction at www.cosip.org where a life demo is currently developed.

UP has been investigating different options for running experiments with resilient services running in virtual machines. PlanetLab is not designed to be used for the testing of virtualized environments. Experimentations trying to avoid this limitation have been realized by using emulation platforms (e.g., Qemu). The results showed that this method is not flexible enough. Therefore PlanetLab is not considered for further resilient services experiments with virtualisation. G-Lab and GpENI are further testbed platforms where UP is considering using them to run service level resilience experiments. Preliminary considerations regarding their relevance to the ResumeNet project is currently work-in-progress. The G-Lab project (started 1. Sept. 2008) has the main objective of enabling autonomous energy efficient management of physical and virtual resources. UP is joining the testbed on Sep. 1st 2009. The first phase will be to set-up 6 nodes of the testbed, out of which three are standard G-Lab nodes and the other three are latest generation Sun nodes supporting energy efficiency features. G-Lab should us allow to manage the services underlying virtualization software with the functionality that is required for the experiments with service resilience in ResumeNet.

[3] http://bamboo-dht.org/

[4] http://entangled.sourceforge.net/

Task 4.4. Resilient smart environments

The testbed to be used has been developed in the context of a French national project (ICOM5). It allows exchanges between applications through heterogeneous hardware and software. This intra - or inter - enterprise infrastructure links various identified objects (RFID, 1D/2D bar codes, NFC, ...) to the company information systems and fixed/mobile terminals and/or, to a lesser extent, the objects to each other.

In ResumeNet the ICOM testbed will be enhanced with respect to the filtering functions and routing information with the use of a PubSub-based platform decoupling message senders and recipients. This platform is based on a network of XML routers using hardware to process messages and allowing very high performance, the network covering itself a network of (traditional) IP routers. The detailed specification of the experimentation scenario is ongoing.

Task 4.5. Cooperating towards a possible federation of testbeds in the FIRE context

This is the only WP4 task that was officially kicked off by the launch of the project and was completed in M18. It is responsible for feeding the FIREworks coordination action with information on the use of experimentation facilities in ResumeNet. Two deliverables have been submitted to FIREworks in M18, one on federation requirements (D4.1b) and one describing the links between experimentation and research in the project (D6.2b). Both constitute updated versions of the deliverables submitted in M6, D4.1a and D6.2a, respectively.

Further to the submission of the deliverables, the FIREworks management requested in M18 more information from the project (more generally, from all FIRE projects) on experimentation but also other aspects such as results and international collaborations. This info has been provided by the ResumeNet Consortium.

2.4.2. Deviation in the time plan and the WP structure from the technical annex

Over the first six months of the 2nd year of the project, partners have continued putting effort on developing further the experimentation scenarios. Hence, some WP4 resources have been used ahead of the official WP launch, which happened on March 2010. The main effort in this WP will anyway be spent during the remaining 12 months of the project lifetime.

5 Infrastructure pour le COMmerce du futur

2.5. WP5: Dissemination and exploitation of projects results and standardization activities

2.5.1. Summary of progress towards dissemination objectives

Publications

The first dissemination activities of this report period are focused on year 2's publications involving, for most of them, an internal collaboration among different ResumeNet's partners. Research work carried out of the project has been presented in scientific journals/magazines and conferences/workshops, as listed below.

Magazines

1. 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)
2. 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

1. 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
2. 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
3. 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
4. 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
5. 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

1. M. Schöller, T. Taleb, and S. Schmid, "Neighbourhoods as an abstraction for fish-eye state routing", IEEE PIMRC, Tokyo, Japan, September 13-16, 2009
2. 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
3. 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

4. T. Taleb, Z. Fadlullah, M. Schöller, and K. Letaif, "A connection stability aware mobility management scheme", IEEE WiMOB, Marrakech, Morocco, October 12-14, 2009
5. 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
6. 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
7. 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
8. 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
9. 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
10. E. Gourdin, "A mixed-integer model for the sparsest cut problem", ISCO 2010, Hammamet, Tunisia, March 24-26, 2010
11. 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
12. M. Fry, M. Fischer, M. Karaliopoulos, P. Smith, and D. Hutchison, "Challenge identification for network resilience", NGI 2010, Paris, France, June 2-4, 2010
13. 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
14. 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
15. 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
16. 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
17. C. Doerr, and J. Martin-Hernandez, "A computational approach to multi-level analysis of network resilience", DEPEND 2010, Venice, Italy, July 18-25, 2010
18. 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
19. 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

20. 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)
21. 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
22. 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
23. 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)

Ongoing work

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

1. 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)
2. 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
3. Jabbar, and J.P.G. Sterbenz, “Towards quantifiable resilience for the future Internet” – submitted to ReArch, Philadelphia, PA, USA, November 30, 2010
4. 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
5. M. Schöller, P. Smith, and D. Hutchison, “Assessing risks for resilient networked systems” – submitted to Journal of Network and Computer Applications, Elsevier
6. 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

Presentations

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

1. 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
2. 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

Further impact-making activities

In addition to the new, significant links developed by the University of Lancaster with two major Telcos (BT and Telekom Malaysia) reported in the previous deliverable D6.4c, 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.

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 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 a PhD student from NUDT as a guest at the Computer Engineering and Networks Laboratory of ETHZ, 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 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 (www.enisa.eu). 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.

2.5.2. Contribution to standardization work

As reported in D6.4b, the inaugural meeting of the "Focus Group on Future Networks", issued from the study group 13 of ITU-T, 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.

2.5.3. Exploitation activities

2.5.3.1. Courses, seminars, theses, research projects

In conjunction with the dissemination activities, ResumeNet academic partners have started to exploit the project results for teaching and (future) research activities. Academic material for undergraduate or graduate courses have been, or will be, elaborated, as well as some seminars are held that contribute to the ResumeNet contents exploitation (see list below).

Undergraduate or advanced courses

- "Computer networks" - Prof. Georg Carle (TUM)
- "Network security" - Prof. Georg Carle (TUM)
- "Peer-to-Peer systems and security" - Prof. Georg Carle (TUM)
- "Computer networking III" - Prof. Hermann De Meer (UP)
- "IT security" - Prof. Joachim Posegga, and Prof. Hermann De Meer (UP)
- "Advances in networking" - Dr. Christian Doerr (TUD)
- "Introduction to IT Security" - Prof. Michael Fry (USyd)
- "Advanced networking course - project work" - Prof. Per Gunningberg (UU)
- "Managing and securing computer networks" - Prof. Guy Leduc (ULg)
- "Network security" - Prof. Bernhard Plattner (ETHZ)
- "Cyber security" – Dr. Daniel Prince, Director of Studies (ULanc)
- “Network security – protocols and architectures” – Dr. Marcus Schöller (Guest Lecturer at Karlsruhe Institute for Technology, Germany)
- "Resilient and survivable networking" - Prof. James P.G. Sterbenz (KU)

Seminars

- "Future Internet" - Prof. Georg Carle (TUM) - selected topics on emerging trends and visions in future Internet research are assessed within this seminar.
- "Innovative Internet technologies and mobile communication" - Prof. Georg Carle (TUM) – this seminar treats selected topics on innovative trends in the context of the mobile Internet.

Theses

Different types of theses, ranging from Bachelor projects to Master or PhD dissertations, and based on the research carried out in the project, have been achieved, or are on the way, as illustrated by the diverse subjects listed below.

Bachelor projects

- Christopher Lambert, "SIP-based enrolment of X.509 certificates" - supervisors: Ali Fessi, and Georg Carle (TUM) – October 2008 / January 2009

- Sascha Päppinghaus, "Support of virtual machine migration using P2P networks" - supervisors: Ali Fessi, and Georg Carle (TUM) – August 2009 / January 2010
- Stefan Peters, "Identification of routing misbehavior in IPv4 networks using the X-Trace framework" – supervisors: Andreas Fischer, and Hermann de Meer (UP) – Spring 2009
- Alexandru Tigaeru, "Dynamic management of logical connections between virtual Xen-Routers" – supervisors: Andreas Berl, Andreas Fischer, and Hermann de Meer (UP) - Winter 2008/2009

Master theses

- Desalegn Abawollo, "Impairment-aware routing" - supervisor: Piet Van Mieghem (TUD) - January 2010 / August 2010
- Matthias Fischaleck, "Discovery of malicious nodes in P2P overlay networks using the X-Trace framework" – supervisors: Andreas Fischer, and Hermann de Meer (UP) – Summer 2010
- Mathias Fischer, "Distributed challenge analysis and remediation in wireless mesh networks - distributed interference minimisation" - supervisors: Paul Smith (ULANC), Merkouris Karaliopoulos (ETHZ), David Hutchison (ULANC), and Bernhard Plattner (ETHZ) – January 2010 / June 2010
- Richard Hartmann, "DHT-based routing for a resilient IP forwarding overlay" – supervisors: Nils Kammenhuber and Georg Carle (TUM) – ongoing work
- Benjamin Hof, "Simulation and analysis of failures in Kademlia" - supervisors: Ali Fessi, and Georg Carle (TUM) – August 2009 / October 2009
- Rasjaad Imamdi, "Robustness analysis and capacity management of the KPN PS mobile core network" - supervisor: Piet Van Mieghem (TUD) – February 2010 / September 2010
- Devender Maheshwari, "Robust offshore networks for oil and gas facilities" – supervisor: Piet Van Mieghem (TUD) – June 2009 / January 2010
- Cliff Maregeli, "A study on TCP-SYN attacks and their effect on a network infrastructure" - supervisor: Piet Van Mieghem (TUD) – December 2009 / July 2010
- Georgios Nomikos, University of Crete, “Resilience of wireless mesh networks to node misbehaviors” – supervisors: Merkouris Karaliopoulos, and Gabriel Popa (ETHZ) – October 2009 / today
- Christian Rothländer, "Robust routing and detour behavior in P2P networks"- supervisors: Ali Fessi, and Georg Carle (TUM) – August 2008 / February 2009
- Sam Tavakoli, "Content-based congestion control in opportunistic networks" - supervisor: Fredrik Bjurefors (UU) - July 2010 / December 2010

PhD dissertations

- Yahya Al-Hazmi, “Resilience in self-organizing virtual networks” – supervisor: Hermann de Meer (UP) - starting date: July 2010
- Azman Ali, “The utility of policies in network remediation techniques” - supervisor: David Hutchison (ULanc)
- Fredrik Bjurefors, "Measurements in opportunistic networks" – supervisor: Christian Rohner (UU)

- Nafeesa Bohra, “Improving resilience using a distributed correlated network monitoring approach” – supervisor: Hermann de Meer (UP)
- Radovan Bruncak, “Applying context information to assist resilience techniques in computer networks” - supervisor: David Hutchison (ULanc)
- Laurent Chiarello, "Combining congestion control and multipath routing in a new Internet architecture", supervisor: Guy Leduc (ULg) – starting date: September 2010
- Ali Fessi, "Resilient application layer signaling based on supervised Peer-to-Peer (P2P) networks" – supervisor: Georg Carle (TUM) – viva planned for end 2010
- Andreas Fischer, “Resilience in a virtualized network environment” – supervisor: Hermann de Meer (UP)
- A. Jabbar, “A framework to quantify network resilience and survivability” – supervisor: J.P.G. Sterbenz (KU), August 2010
- Andreas Louca, “Towards an autonomic infrastructure for network resilience” - supervisor: Andreas Mauthe (ULanc)
- Angelos Marnerides, “Anomaly classification techniques for resilient networks” - supervisor: David Hutchison (ULanc)
- Javier Martin Hernandez, "Robustness of complex networks" – supervisor: Piet Van Mieghem (TUD)
- Rim Moalla, "Service resilience – detection, remediation and recovery" – supervisor: Chidung Lac (FT) – starting date: November 2010
- Jasmina Omic, "Epidemics in networks: modeling, optimization and security games" – supervisor: Piet Van Mieghem (TUD)
- Gabriel Popa, " Fostering cooperation in decentralized networks with (un)correlated data sources " – supervisor: Bernhard Plattner (ETHZ)
- Yue Yu, "Distributed challenge detection" – supervisor: M. Fry (U. of Sydney)

2.5.3.2. Research results exploitation

- A Intra-European Marie Curie Fellowship (MC IEF) resulted from research initiated within the context of the ResumeNet project. The proposal was submitted in response to the FP7-PEOPLE-2009-IEF Call of the People Marie Curie actions (deadline: 18 Aug 2009) by Dr. M. Karaliopoulos and University of Athens, Greece, as Host Institution. The title of the proposal is: “Resilience of opportunistic networks to node misbehaviors (Retune)” and has been inspired by work carried out by the researcher during the first year of the project in the context of WP2. The proposal was selected for funding with the amount of 188 k€ for 2 years; the starting date of the Fellowship is September 1st 2010.
- The part-time chair "Robustness of Complex Networks", held by Prof. Robert Kooij (TUD), aims to quantify the robustness of complex networks under various types of attacks and/or failures. The research done within ResumeNet on this subject has made it possible for the chair to apply the robustness concept in various multidisciplinary settings.

2.5.3.3. Industrial exploitation plans

France Telecom-Orange, through a press conference made in July 2010, has presented a five-year action plan, called "Conquests 2015", which aims at setting out the challenges and perspectives that lie ahead, and clarifying the Group’s business activities. Among the four

strategic directions, the one about the "conquest of networks" can take full advantage of ResumeNet research results. Actually, one key point of this development axis is the continued improvement of network service quality, by giving more intelligence, power, and reliability to the operator's networks. Following this 2010-2015 action plan, ResumeNet definitively serves FT's ambition to become Europe's telecom service provider of reference, and particularly a reference for service quality in future networking. Actually, besides traditional performance criteria, technical QoS metrics are based both on dependability (availability, reliability, etc.), and security. These two main components of networks and services resilience, studied in ResumeNet, will provide practical results a Telco can exploit to strengthen its networks (part of the nation's critical infrastructures), and differentiate its commercial offers from the competitors' ones.

Within this consortium, the manufacturer NEC will be made aware of the operators' adapted and new business models, thus they will be well positioned for serving this new demand in a market that is not only shifted but also enlarged. The approach of ResumeNet does not necessarily imply that there will be a disruption of the business models; however, these will be shifted, not only due to the technology itself but also due to continuing trends (like virtualised networks or in network management). Products based on technologies developed with a resilience focus will meet a market demand, provided they offer superior performance and economy. Moreover, the project offers an early research and technology transfer from the universities to the industrial partners of the project. Disaster proof networking is an important issue for network operators in many areas. Especially in seismic active areas, like Japan, technologies to reliably operate distributed systems under very challenging conditions are demanded. This affects all kind of network operations, from 3G mobile networks, backbone networks, distributed data-centre, and cloud networks. All these systems have in common that high availability of the services provisioned over a networked infrastructure is requested by the customers. The results of the ResumeNet project allow NEC to strengthen its position in this market by augmenting the feature set of future products.

2.5.1. Deviation in the time plan and the WP structure from the technical annex

No deviation from the work planned in the DoW is to be reported during the second year of ResumeNet WP5 activities.

3. Deliverables and milestones tables

3.1 Deliverables (excluding the periodic and final reports)

Table 3.1: Deliverables

Del. no.	Deliverable name	WP no.	Lead beneficiary	Nature	Dissemination level	Delivery date from Annex I	Delivered	Actual / Forecast delivery date	Comments
1.1	Understanding of challenges and their impact on network resilience	1	NEC	R	PU	M6	✓	22/10/2009	Delivered before end of M7 to allow inclusion of risk-assessment approach in the document.
1.2a	Defining metrics for resilient networking (Interim)	1	TUDelft	R	PU	M18	✓	26/02/2010	Delivered on time
1.3a	Politics for resilience (Interim)	1	NEC	R	PU	M18	✓	18/03/2010	Delivered with a short delay
1.4	Cross-layer optimization and multilevel resilience	1	ULANC	R	PU	M24	✓	15/10/2010	Delivered with a short delay
1.5a	First interim strategy document for resilient networking	1	ULANC	R	PU	M12	✓	05/10/2010	Delivered with a short delay
1.5b	Second interim strategy document for resilient networking	1	ULANC	R	PU	M24	✓	24/09/2010	Delivered with a short delay
2.1a	First draft on defensive measures for resilient networks	2	FT	R	PU	M15	✓	05/12/2010	Delivered with a short delay

Table 1. Deliverables (continued)

Del. no.	Deliverable name	WP no.	Lead beneficiary	Nature	Dissemination level	Delivery date from Annex I	Delivered	Actual / Forecast delivery date	Comments
2.1b	Defensive measures for resilient networks	2	TUDelft	R	PU	M24	✓	20/09/2010	Delivered with a short delay
2.2a	First draft on new challenge detection approaches	2	ULg	R	PU	M18	✓	05/03/2010	Delivered with a short delay
2.2b	New challenge detection approaches	2	ULg	R	PU	M24	✓	24/03/2010	Delivered with a short delay
2.3a	First draft on the remediation, recovery, and measurement framework	2	ULANC	R	PU	M18	✓	05/03/2010	Delivered in time
2.3b	Remediation, recovery, and measurement framework	2	NEC	R	PU	M24	✓	24/03/2010	Delivered with a short delay
3.1a	Taxonomy of P2P, Overlays and Virtualization techniques with respect to service resilience	3	UP	R	PU	M12	✓	02/10/2009	Delivered with a short delay
3.1b	Resilient Service Architechture	3	TUM	R	PU	M20	✓	11/05/2010	Delivered with a short delay
3.2	Service Surveillance	3	FT	R	PU	M22	✓	20/07/2010	Delivered with a short delay

Table 1. Deliverables (continued)

Del. no.	Deliverable name	WP no.	Lead beneficiary	Nature	Dissemination level	Delivery date from Annex I	Delivered	Actual / Forecast delivery date	Comments
3.3	P2P overlays and virtualization for service resilience	3	TUM	R	PU	M24	✓	20/09/2010	Delivered with a short delay
4.1a	Federation Requirements (Interim)	4	ETHZ	R	PU	M6	✓	09/04/2009	Light deliverable in response to the delayed request for inputs from FIREWorks
4.1b	Federation requirements (Final)	4	ETHZ	R	PU	M18	✓	26/03/2010	Delivered with a short delay
4.2a	Interim report on experimental evaluation of resilient networking	4	UU	R	PU	M24	✓	08/10/2010	Delivered with a short delay
5.1	ResumeNet website and Wiki pages	5	ETHZ	O	PU	M2	✓	10/2008	Delivered in time
5.2a	Yearly reports on dissemination activities	5	ULANC	R	PU	M12	✓	02/10/2009	Delivered in time
5.2b	Yearly reports on dissemination activities	5	ULANC	R	PU	M24	✓	20/09/2010	Delivered with a short delay
5.3a	Exploitation Plans (Interim)	5	FT	FT	PU	M24	✓	24/09/2010	Delivered with a short delay
6.1	Project Management Guidelines	6	ETHZ	R	PP	M2	✓	31/10/2008	Delivered in time

Table 1. Deliverables (continued)

Del. no.	Deliverable name	WP no.	Lead beneficiary	Nature	Dissemination level	Delivery date from Annex I	Delivered	Actual / Forecast delivery date	Comments
6.2a	Links between research and experimentation (Interim)	6	ULANC	R	PU	M6	✓	09/04/2009	Light deliverable in response to the delayed request for inputs from FIREWorks
6.2b	Links between research and experimentation (Final)	6	ULANC	R	PU	M18	✓	03/04/2009	Delivered with a short delay
6.3	Report on technical work in WP2 and WP3 during first year	6	ETHZ	R	PU	M12	✓	05/10/2009	Delivered with a short delay

3.2 Milestones

Table 3.2 Milestones

#	Milestone name	Work package no	Lead beneficiary	Delivery date from Annex I	Achieved Yes/No	Actual / Forecast achievement date	Comments
1.1	First view on resilience metrics and classes definition	1	TUDelft	M18	Yes	M18	Deliverable D1.2a
1.2	Policy definition and SLA-like resilience requirements formulation	1	NEC	M18	Yes	M18	Deliverable D1.3a
2.1	First demonstrator of the optimization tool for resilient network topologies	2	FT	M22	Yes	M22	Software on SVN
2.2	First Prototype of the Adaptation and Evolution Framework	2	NEC	M24	Yes	M24	Software on SVN
3.1	Specification of the role of P2P overlays and virtualization in providing resilient services	3	TUM	M24	Yes	M24	Deliverable D3.3
5.1	Website and Wiki pages set up and operational	5	ETHZ	M2	Yes	M2	

4. Project management

The basic concern of the management team for the second year of the project lifetime was to make the appropriate changes and take measures in response to the comments it obtained in the first year review of the project. The review meeting took place in Zurich end October 2009; the project got positive comments and all its deliverables were accepted. The main request from the reviewers was to ensure close integration of partners' efforts in the years 2 and 3 of the project lifetime.

Besides leveraging the available management tools and processes (meetings, Wiki, emailing lists) for fostering collaboration, there has been persistent effort from the management team to put the partners work even closer together. This is clearly favored by the progress of the project research agenda in the year 2, where the combined effort of partners is mandatory to fulfil the project objectives. In parallel, a) the recommendations of the reviewers have been promoted to distinct progress monitoring checkpoints; b) monitoring tools have been put in place to track all areas where partners make joint efforts.

An issue that became subject of extensive discussion in the Consortium is the project approach to experimentation. There was a recommendation from the reviewers to try to integrate some of the four experimentation scenarios in favor of a "fatter" scenario that could probably show more aspects of the framework and the mechanism working together. These discussions led to the organization of a separate meeting on March 16th in Zurich, where three options with respect to experimentation were discussed exhaustively: a) introduce a new single "fat" experimentation scenario; b) combine one or more of the existing experimentation scenarios into a "fatter" one; c) stick to the current approach with four experimentation scenarios and load them with additional features, where possible and appropriate.

The Consortium decided to adopt as baseline the third option with a parallel commitment of the partners involved in the experimentation scenarios to fully detail and revise them by the next plenary meeting of May 17th, in Uppsala, Sweden. There, a definite decision was made on the experimentation approach, after getting the thorough view of the four experimentation scenarios. Among others, it was argued that the four scenarios would help demonstrate the applicability of the project approach to many different scenarios and that many of them bring together elements of work from various project research areas, having already strong integration elements themselves.

Other tasks of the project management during this year included:

- Maintaining synchronization of the whole Consortium about the project activities. Management issues, communication at the scientific level and synchronization of the work between all partners was mainly achieved through bi-weekly phone conferences (every other Thursday) and emails through the ResumeNet mailing lists. Minutes of the phone conference were made available to all consortium members via the internal part of the project website, which has been constantly been updated throughout the last six months. Additionally, the WP-level regular phone conferences were intensified for WP1- WP3 with parallel task-level PhCs.
- Project monitoring. Project processes (deliverable preparation, milestone fulfilment) were monitored according to the surveillance processes established during the first year of the project lifetime. One positive result out of this process was the respect of deliverables' delivery dates. Out of the 18 deliverables that were submitted to EC, there was no case that the hard deadline of 45 days after the official deliverable delivery date was exceeded. In fact, all deliverables were submitted within less than a

month after their official delivery date, with more than half of them delivered with less than a two-week delay.

- Organization of physical meetings. To monitor and coordinate the overall project work and also for discussion and workshops within individual WPs, three plenary meetings took place during the past half year: the third plenary meeting in Munich, Germany, 7-9 October 2009, the fourth plenary meeting in Delft, NL, 20-22 January 2010 and the fifth plenary meeting in Uppsala, 17-19 May. All plenary meetings have been combined with separate meetings of the Project Technical Committee, which lasted half a day and take place on the afternoon before the first day of the plenary meeting. The list of meetings that are scheduled for the next 6 months of the project is given in Table 4.1.
- Meeting with the Advisory Board: The Paris project meeting was combined with a meeting with the project Advisory Board members. Two of them were physically present there (Dr. Rick Schlichting, and Prof. Jim Kurose). The third member, Prof. Rüdiger Grimm, could not join because he had other obligations during this time. The Consortium obtained a range of excellent and supportive comments from the advisory board members.
  The fourth member of the Advisory board, Dr. Jean-Claude Laprie**,** couldn't be present during the meeting because he was ill. It was with great sadness that we learned shortly after the meeting that he passed away on October 17, 2010. We are indebted to Jean-Claude for the clear and well thought-out advice that we had the privilege to receive from him. We will always keep a fond and respectful memory of this first-class scientist, who laid the ground for much of the work we are carrying out in this project. His dependability work is seminal, and constitutes the basis for the architectural formalisms that we have adopted in ResumeNet.

Table 4.1: Physical meetings envisaged over the next 6 months of the project

Meeting	Context (scope)	Date	Location/ Host
6th Project plenary meeting	The tri-annual plenary project + Advisory Board meeting	28 Sept – 1 Oct 2010	Paris, France
2nd annual review meeting	Review meeting + brief project TPM group meeting to plan work after the review	4 Nov 2010	Brussels, Belgium
7th Project plenary meeting	Project technical progress review meeting	Jan 2011	Liège, Belgium

4.1 Changes in the composition of the project management team

During year 2 of the project lifetime, there have been two noteworthy changes with respect to the persons involved in the management of the project.

- In December 2010, Dr. Regina Notz from the Euresearch team of ETH Zurich replaced her colleague Mrs. Sibylle Hodel in the provision of administrative support to the project management. She has taken an active role in the several project management

tasks and has been instrumental in preparation of deliverables, meetings and this project report.

4.2 Proposed changes to the Description of Work for Y3

The Project Management Team in agreement with the ResumeNet PCC proposes a number of changes to the DoW for the third and last year of the ResumeNet project. These modifications concern shifts of resources between partners, changes in the WP and project management team, extension of task 2.1 and some formal shifts between budget categories. These changes are described in a separate paper and will be discussed at the review meeting of November 4th, 2010 in Brussels.

5. Explanation of the use of the resources

Omitted from this version of the deliverable.