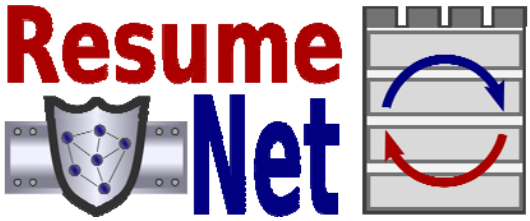
Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation



3rd Periodic Progress Report (September 2009 – February 2010)

PROJECT PERIODIC REPORT

Grant Agreement No.	224619
Project title	Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation
Deliverable number	D6.4c
Deliverable name	3rd Periodic Progress Report
WP number	6
Delivery date	31 March 2010
Actual delivery date	16 April 2010
Editor	M. Karaliopoulos, R. Notz (ETHZ)
Contributors	A. Fessi (TUM), M. Karaliopoulos (ETHZ), C. Lac (FT), M. Schöller (NEC), P. Smith (ULANC)
Reviewer	M. Schöller (NEC)

Publishable summary

The work 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 requirements from resilient networks are 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 resilient networks' operation, whereas Diagnose and Refine compose the outer, longer-term control loop. The six strategy components could be easier conceptualized with the help of the castle metaphor:

- *Defence*, according to which the Internet is made robust to challenges and attacks (analogy: strong castle wall);
- *Detection* of an adverse event or challenge that has impaired normal operation of the Internet and degraded services (analogy: guards on the castle wall);
- *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);
- *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);
- *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
- *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).

For a network to be able to carry out these six operations, we need a good understanding of several concepts. This work is undertaken within ResumeNet 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 cross-layer mechanisms for collecting and sharing information from different layers to enable detection and remediation actions.

The project work over the first half of the project lifetime has covered all four main elements that have to be well understood and defined for realizing the framework, i.e., challenges, metrics, policies, and *cross-layer mechanisms* for information sensing and sharing among protocol layers. The level of progress is each direction varies, with the work on challenges and metrics being more advanced than that on policies and cross-layer mechanisms.

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. More work needs to be done to accommodate, in a scalable manner, the multi-level resilience aspects.

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, work so far on cross-layer information sharing in various directions. First, the use of context information to better inform detection and remediation strategies is studied. Secondly, X-the use of X-Trace as a tool to enable sharing of information among layers within a node but also among different nodes is jointly studied by University of Passau and University of Lancaster. Finally, on a more case study note, University of Lancaster and Kansas University are collectively implementing an error control scenario in ns-3, where various error control mechanisms, e.g., FEC or ARQ, can be implemented on a hop-by-hop or end-to-end basis. The aim of implementing this scenario is to investigate the trade-offs associated with performing error control in different ways, given distinct application requirements.

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

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.

Five different defensive measures are pursued 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. 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 two main thrusts, first the identification and characterization of multiple reliability modes, and second Path Diversification, a heuristic approach to selecting multiple end-to-end paths for simultaneous or failover use. The fourth approach is looking at “QoS2: Integrating QoS with Quality of Security”. This defensive measure balances quality of service versus quality of security. The fifth defensive measure investigates the required protection each node has to provide to protect the overall system from malware spread. This activity is called “Protection against malicious information spread”.

Since challenge detection has been a research topic for several years, an extensive literature study and consolidation effort had to be performed first. Based on these results, ResumeNet partners pursued three 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 a distributed information storage and sharing infrastructure to support challenge detection and fault analysis.

Finally, ResumeNet partners have investigated three different scenarios to extract requirements for the system remediation (and, to a longer term, adaptation (functionality): 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 have 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.

WP3, launched in parallel with WP2, investigates different resilience mechanisms which are complementary to WP2. The focus in this WP is on the application layer. Hereby, the 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 lookup service; b) overlay-based end to end connectivity; and c) virtualisation.

P2P lookup is used to provide resilient lookup of a communication partner, e.g., for VoIP call, or a web session. Thus, we are currently investigating the drawbacks of existing signalling solutions for this purpose, particularly DNS and SIP, and how to build resilient alternatives using concepts learned from P2P networking. If the communication between the two end points is disrupted, then overlay-based end-to-end connectivity comes into place, where a P2P overlay network[1] is used for providing end-to-end connectivity as a failover. Virtualisation is another key technology to provide resilient network services. 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. Hereby, the costs and implications of different migration techniques are currently being investigated.

While work in WP3 has a strong focus on proactive resilience mechanisms, it is still always required to monitor the health of the network and the provided services on top and detect challenges when they occur. In this WP, localisation strategies of monitoring probes have been investigated. The correlation of events is planned to occur using the FT’s Chronicle Recognition System (CRS). The usage and integration of these activities on monitoring and challenge detection with other activities, such as challenge detection in WP2, and policies and cross-layer information

[1] Eventually another P2P network, since lookup and end to end connectivity are different goals with different requirements, e.g., DHT routing algorithms are suitable for data lookup while end to end connectivity would require a different approach for routing, e.g., link state routing.

exchange in WP1 is an ongoing work. With the Detection, all four steps in the inner loop of the ResumeNet resilience strategy (D^2R^2) are realized at the service level. Work on Diagnose and Refine is currently not planned.

The evaluation of both principles and mechanisms is carried 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 analog, Planetlab Europe).

During the first half 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. Although WP4 work officially starts in M18, both test beds (in the case of TikNet) and experimentation scenarios (study cases 1-2, 4) have been defined in higher detail, whereas for experimentation study case 2, preliminary experiments have already begun. In parallel, the activities in WP4 have supported the activities of the EU FIREWorks Coordination Action[2] via compilation of two versions of two light deliverables on the federation requirements and the links between research and experimentation in ResumeNet.

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 test beenabling trusted access to e-Services.

With this in mind, ResumeNet has devoted considerable effort in the first one and half year to the dissemination of its results:

- 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.
- ResumeNet has been presented, with the use of flyers, posters[3], or slide sets, in various venues including magazines (ERCIM journal); scientific conferences and workshops (IWQoS 2008 Conference, IWSOS 2008 Workshop); events organized by the European Commission (SAC/FIRE Workshops, FIRE Launch Event, ICT 2008). In the same time, significant work carried out within the project or during the project bidding and preparation phases 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.

[2] http://www.ict-fireworks.eu/
[3] The latest version of ResumeNet's poster is available now in the public Web site.

- 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. It is always keen to support standardization actions originating from these bodies and federating the European industry sector. Nevertheless, 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").
- A Dagstuhl Seminar on "Architecture and Design of the Future Internet" was organized by Georg Carle, David Hutchison, Bernhard Plattner, and James 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. Network resilience and the ResumeNet approach to it attracted significant share of the overall discussion over the three days of presentations and forum-like interactions.

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 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 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. With ANA, in particular, a joint workshop was held on June 12th 2009 in Lancaster, UK, before the 2nd plenary meeting of the project. The aim was to identify what ANA outcomes could be reused and can benefit the work in ResumeNet.

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).

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 period

The project activities during the first half of the second year were focussed on two main objectives:

Making progress in research on network resilience framework and mechanisms: the major research efforts in the project were made, as planned, in 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 and D1.3a, scheduled for M18, were intended to describe the outcomes of this effort.

Moreover, considerable work was planned for WP2 and WP3, where the first two capabilities of the short-term control loop in the D2R2+DR framework, i.e., Detection and Remediation, were to be investigated and reported. The interim deliverables D2.2a and D2.3a were scheduled for M18 as summaries of our up-to-date understanding of these two framework capabilities.

Strengthening the integration of partners' effort in the project: being closely related to the first project objective, 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 start at M18, it was decided to foster more integration during the first six months of year 2 by focussing on the first approach. Nevertheless, there have also been several discussion rounds with respect to the second, experimental, approach towards further integration.

These two 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, they requested:

- 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.
- Better linking of the research work to the overall framework concepts and promotion of the cross-layer and distributed nature of resilience.
- Leverage and validation of the results on archived traces and/or live network data, with a call for relevant contributions from industrial partners.

With respect to dissemination, the aim was to disseminate the first project results in places (conferences and workshops), where prompt feedback could be obtained.

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

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

During this period a number of advances in the understanding of the ResumeNet resilience architecture were made that fed into various deliverables, in particular, those in WP1. A manifestation of this new understanding resulted in a new diagrammatical representation of the strategy, which has proven useful for presenting the project's results in the context of the strategy. Specifically, we began to explore the complexities of configuring the various mechanisms that can be used to enable resilience, identifying, for instance, the potential conflicts that lie along the D^2R^2+DR strategy, and across multiple layers of the protocol stack. This thinking was utilised in the paper that was submitted to AIMS 2010, and formed part of D1.3a, described below. Furthermore, we have begun to explore a realization that cross-layer information sharing should be generalised to consider the use of context, which is informing work that is being undertaken in T1.5. Many of these findings will be described in D1.5b, which is due in M24 of the project.

A significant outcome from T1.1 activities is a lead publication to a special issue on resilient and survivable networks that provides a survey on related disciplines, and describes the resilience framework, including the strategy and principles, which form the basis for the ResumeNet project.

Task 1.3: Resilience metrics

Significant effort in this quarter has gone into the delivery of D1.2a, the first interim deliverable on resilience metrics. In the deliverable, we present continuing work on the development of a general framework for assessing the robustness of a system. In the context of a number of topological scenarios, i.e., the U.S. telecom operator Sprint and the European research network GEANT2, we conducted a study of the approaches we are considering for quantifying resilience. The aim of study was to implement, test and investigate the utility and potential shortcomings of the concepts of resilience quantification discussed in the deliverable, and verify the outcomes of two analysis approaches we are investigating against each other. We introduce in this deliverable our intentions with regard to exploring the use of resilience classes to help address the issue of complexity when specifying and realising mechanisms to meet resilience requirements. This deliverable will be completed with its final version, which is due M36 of the project.

Task 1.4: Policy specification for resilience

This task within the project aimed to investigate how policy-based management frameworks could be applied to configuring the various mechanisms for resilience, such as detection and remediation mechanisms. This investigation culminated in findings that are described in D1.3a and in a publication submitted to the AIMS 2010 conference. In short, in D1.3a, we 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.

In the 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. Furthermore, we discussed some of the complexities of defining concrete configurations of resilience mechanisms from high-level requirements, and how the state-of-the-art in policy-based management techniques could be applied in order to address these complexities.

D1.3 will be re-visited at the end of the project to detail the lessons learned from applying policy-based management techniques to the resilience architectures that are being developed in Work Packages 2 and 3.

Task 1.5: Cross-layer optimization and multi-level resilience

Our work in this task on understanding the various approaches to cross-layering continues. Specifically, Uni. Lancaster and Kansas Uni. are collectively implementing an error control scenario in ns-3, where various error control mechanisms, e.g., FEC or ARQ, can be implemented on a hop-by-hop or end-to-end basis. The aim of implementing this scenario is to investigate the trade-offs associated with performing error control in different ways, given distinct application requirements.

Also, as part of our effort to understand the importance of multi-level information sharing (and control, as described above), we have begun to think more broadly about the use of context information to better inform detection and remediation strategies. For instance, if it is understood that a particular event is occurring at a given time, we can use this information to inform detection and remediation, e.g., identify a challenge as a flash crowd, rather than a DDoS attack. Our earlier work on determining the state-of-the-art in cross-layer information sharing has been extended to consider how context could be used.

Finally, a new initiative has begun with Uni. Passau on how X-Trace can be used to provide cross-layer information, as a form of context information, to enable improved detection and remediation. At the time of writing, this activity was just getting underway, with discussions regarding the scope of the activity and potential scenarios being discussed.

WP1 main output

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

- A lead paper to a special issue on resilient and survivable networking, regarding related resilience disciplines and the resilience strategy.
- Delivery of two interim deliverables: D1.2a on resilience metrics and D1.3a on policies for resilience.
- A paper submission to AIMS 2010 conference regarding the application of policies to the problem of defining configurations for resilience.

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

There have been no significant deviations from the time plan, as described in the technical annex.

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 that 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. 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 two main thrusts, first the identification and characterization of multiple reliability modes, and second Path Diversification, a heuristic approach to selecting multiple end-to-end paths for simultaneous or failover use. The fourth approach is looking at “QoS2: Integrating QoS with Quality of Security”. This defensive measure balances quality of service versus quality of security. The fifth defensive measure

investigates the required protection each node has to provide to protect the overall system from maleware. This activity is called “Protection against malicious information spread”.

The state of the art, the approach to these measures and first results are presented in Deliverable D2.1a. It was finalized and submitted in M15 and will be updated by the end of the second project year (M24).

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 three 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 state of the art, the approach to these measures and first results are presented in Deliverable D2.2a. It was finalized and submitted in M18 and will be updated by the end of the second project year (M24).

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 investigates system evolution and refinement of the resilience architecture. 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.

The state of the art, the approach to these measures and first results are presented in Deliverable D2.3a. It was finalized and submitted in M18 and will be updated by the end of the second project year (M24).

WP2 main output

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

- Delivery of three interim deliverables: D2.1a on defensive measures, D2.2a on challenge detection, and D2.3a on the resilience framework.
- Eleven papers attached to D2.1a on defensive measures
- One paper attached to D2.2a on challenge detection
- Three papers attached to D2.3a on the adaptation framework
- Three additional publications from WP2 partners which are not reported in the deliverables yet, and three publications submitted for review

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

There have been no significant deviations from the time plan, as described in the technical annex.

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.

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 can P2P networks can be used for building resilient services. Hereby, two types of architectures have been considered:

- An architecture where services are provided not only by a provider infrastructure but also by the end hosts. Here, we focus on VoIP as an example of a service, as telephony is a critical service which needs to be protected particularly in case of large scale disasters; and as the PSTN is being replaced with VoIP. The signalling protocol used is SIP. In this task, we have investigated the combination of server-based SIP signalling together with P2P SIP signalling as a backup in order to benefit from the advantages of both approaches. Our solution is called Cooperative SIP (CoSIP). Since security is inherent to resilience, we need to address the security issues raised by decentralised solutions such as P2P SIP and in particular CoSIP. In the last half year we have been working on privacy-related issues. Both P2P SIP and CoSIP raise location privacy and other social privacy issues which have been addressed. The results have been documented in a paper submitted to ACM IPTComm 2010.
- An architecture where services are provided by an infrastructure. In this case, our goal is to increase the availability of the service lookup, i.e., probability that a client can successfully find a server providing the required service. In case a client is already connected to a server, which is being migrated (potentially over the Internet), our goal is also to keep the connectivity between server and client as long as possible. The latter activity has been carried in cooperation between TU Munich and University of Passau (see also Task 3.3). As we investigate a resilient service lookup here, we need to compare our work with the most prominent protocol currently used in the Internet for service lookup, namely DNS. In the last half year, we have been investigating the qualities and shortcomings of DNS, and how to overcome the shortcomings with a P2P-alike solution. Our approach for a P2P DNS system differs from earlier approaches in this direction in several aspects, which will be described in the appropriate upcoming deliverables in WP3 and upcoming publications. One of the main differences is that we consider a novel overlay topology (instead of simply using an existing one, such as Chord or Pastry as in previous work on P2P DNS) which which can achieve a low diameter (2-3 hops). The motivation is to build a service lookup solution which provides not only resilience under adverse conditions, but also a low performance stretch compared to the current DNS.

Task 3.3: Management and security of virtualization services

Uni Passau contributed to WP3 by investigating the migration of virtual services. Identifying the cost for different service migration techniques has been determined as a critical requirement for implementing optimal remediation. By identifying the different components contributing to the overall cost of service migration (e.g. service downtime, used bandwidth ...). Uni Passau expects to be able to compare the impact of migration alternatives. To that end, several migration techniques have already been proposed and will be evaluated. Work has progressed already on using network virtualization techniques to enable service discovery after migration.

Task 3.4: Service surveillance and detection of challenging situations

The aim of this task is to build a framework for monitoring any service requiring a certain level of resilience. To this end, probes need to be inserted at the proper location, and their outputs, called alarms, should be analyzed and treated using a correlation engine. The outcome of this analysis, i.e., a challenge detection called alert, will trigger remediation with the help of policies deployment/modification.

A study of basic monitoring principles has been realized, focusing on the organization of management infrastructures, the identification of monitoring policies, and some maintenance operations. The correlation engine we propose to work on is based on chronicles recognition. A review of chronicles used for intrusion, or dependability-related failure detection has also started.

Finally, the application of access policies defined in D2.3a (see 4.2.1) has been sketched in the framework of the experimentation scenario "Communicating objects' data platform" described in D4.1b, which will constitute the service use case for this task.

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

This task aims at providing end-to-end connectivity using an overlay as a failover technique in case of disruption of IP connectivity. Progress in Task 3.5 can be summarised as follows:

- Conducted detailed requirements analysis for Task 3.5
- Laid out architectural draft for Task 3.5
- Continued prototypical implementation for IP-based overlay in SSFNet simulator
- Performed survey on similar software packages that can be used as starting points for building the forwarding overlay on top of them: n2n (distributed VPN), tinc (distributed VPN), SPoVNet Ariba (generic mechanism for constructing overlays), RON (IP overlay), GNUnet with added IPv6 layer (distributed secure P2P network)

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. The search for a replacement, still continuing, has not succeeded yet. The work in Task 3.4 is thus delayed. As a consequence, D3.2 (Service Surveillance), due in June 2010 (M22), will be 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).

WP3 main output

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

- Investigated privacy issues raised by resilient P2P VoIP solutions, and submitted a paper to ACM IPTComm 2010.
- Performed an analysis of the DNS resilience and investigated appropriate overlay topologies for a resilient alternative.
- Evaluation of the implication of migration of services running in virtual machines
- Work on monitoring and challenge detection has continued
- Performed state-of-the-art analysis and laid out architecture for overlay-based end-to-end connectivity.

2.4. WP4: Experimentation with 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. Each one assesses a subset of the D^2R^2+DR strategy aspects and the concepts/mechanisms realizing it.

Although work on experimentation begins in the second half of the project lifetime, significant effort has been devoted so far 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 deliverables D4.1b and D6.2b, 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 node should remain fairly low as long as the throughput requirements from other stations remain also low.
- Making a set of modifications to a known shortest path routing protocol (such as OLSR), whose role would be to provide information about dependencies created by data streams between nodes to all networked stations.
- A software module running on each individual machine for computing the communities of cooperating nodes and responding to changes in the level of cooperation.

Task 4.2. Resilient forwarding in opportunistic networks

Our experimentation is two-fold. We investigate the impact of node misbehaviors 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. The Xen virtual machine monitor is at the core of the testbed. Xen supports execution of multiple guest operating systems (or emulated Haggle devices), on a single physical machine, that are monitored by a host system.

Additional work in ResumeNet will concern the development of modules related to the implementation of node misbehaviours. The work so far has addressed the definition of the service scenario. The current thinking is to use as reference the push-based system developed in Haggle for data delivery. Some first selfishness and attack scenarios have been identified 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[4], which is in Java to a Kademlia implementation in Python called Entangled[5], 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.

Task 4.4. Resilient smart environments

The testbed to be used has been developed in the context of a French national project (ICOM[6]). 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 were 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

[4] http://bamboo-dht.org/
[5] http://entangled.sourceforge.net/
[6] Infrastructure pour le COMmerce du futur

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 these 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 18 months of the project lifetime.

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

2.5.1. Summary of progress towards objectives

The main dissemination activities during this report period are focused on publications involving, for some 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.

Journals

• M. Karaliopoulos, “Assessing the vulnerability of DTN data relaying schemes to node selfishness,” IEEE Communication Letters, vol. 13, no 12, December 2009, pp.923-925

• Z. Fadlullah, T. Taleb, A. V. Vasilakos, M. Guizani, and N. Kato, “DTRAB: Combating Against Attacks on Encrypted Protocols through Traffic-Feature Analysis”, accepted - to appear in ACM/IEEE Transactions on Networking, 2010

• M. Sifalakis, M. Fry, and D. Hutchison, “Event detection and correlation for network environments”, accepted - to appear in IEEE Journal on Selected Areas in Communications, Special Issue on “Recent Advances in Autonomic Communications”, 2010

• 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”, accepted - to appear in Computer Networks (COMNET), Special Issue on Resilient and Survivable Networks, Elsevier, 2010

• T. Taleb, and K. Ben Letaief, “A Cooperative Diversity Based Handoff Management Scheme”, IEEE Transactions on Wireless Communications, Vol. 9, No. 4, April 2010

Magazines

• A. Berl, A. Fischer, and H. de Meer, "Virtualization in the future Internet - virtualization methods and applications", Informatik-Spektrum - Issue on Future Internet, Springer-Verlag, Vol. 33, No. 2, 2010, pp. 186-194 (in German)

• N. Kammenhuber, A. Fessi, and G. Carle, “Resilience of the Internet against disruptions – state of the art in R&D", Informatik-Spektrum - Issue on Future Internet, Springer-Verlag, Vol. 33, No. 2, 2010, pp. 131-142 (in German)

Conferences

• M. Schöller, T. Taleb, and S. Schmid, “Neighborhoods as an abstraction for fish-eye state routing”, IEEE PIMRC, Tokyo, Japan, September 13-16, 2009

• F. Hugelshofer, P. Smith, D. Hutchison, and N.J.P. Race, “OpenLIDS: a lightweight intrusion detection system for wireless mesh networks”, 15th Annual International Conference on Mobile Computing and Networking (MobiCom), Beijing, China, September 20-25, 2009

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

• G. Popa, F. Legendre, E. Gourdin, “Topological Conditions for Collaboration in Wireless Mesh Networks”, Poster at 4th IFIP International Workshop on Self-Organizing Systems (IWSOS 2009), Zurich, Switzerland, December 9-11, 2009

• E. Gourdin, "A Mixed Integer Model for the Sparsest Cut Problem", International Symposium on Combinatorial Optimization (ISCO), Hammamet, Tunisia, March 24-26, 2010

• J.P.G. Sterbenz et al., “The Great Plains Environment for Network Innovation (GpENI): A Programmable Testbed for Future Internet Architecture Research”, 6th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (TridentCom), Berlin, Germany, 18–20 May 2010

• M. Schöller, P. Smith, C. Rohner, M. Karaliopoulos, A. Jabbar, J.P.G. Sterbenz, and D. Hutchison, "On Realising a Strategy for Resilience in Opportunistic Networks", Future Network and Mobile Summit 2010, Florence, Italy, 16-18 June 2010

Workshops

• 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 Modeling (RNDM), St. Petersburg, Russia, October 12-14, 2009

• J.P. Rohrer, A. Jabbar, and J.P.G. Sterbenz, “Path diversification: a multipath resilience mechanism”, 7th IEEE International Workshop on the Design of Reliable Communication Networks (DRCN), Washington, DC, USA, October 25-28, 2009

• C. Auer, P. Wüchner, and H. de Meer, "The degree of global-state awareness in self-organizing systems", 4th International Workshop on Self-Organizing Systems (IWSOS), Zürich, Switzerland, December 9-11, 2009

• W. Elmenreich, R. D'Souza, Ch. Bettstetter, and H. de Meer, "A survey of models and design methods for self-organizing networked systems", 4th International Workshop on Self-Organizing Systems (IWSOS), Zürich, Switzerland, December 9-11, 2009

• C. Doerr, P. Smith, and D. Hutchison, "Network heterogeneity and cascading failures - an evaluation for the case of BGP vulnerability", 4th International Workshop on Self-Organizing Systems (IWSOS), Zürich, Switzerland, December 9-11, 2009

• R. Holzer, and H. de Meer, "Quantitative modeling of self-organizing properties", 4th International Workshop on Self-Organizing Systems (IWSOS), Zürich, Switzerland, December 9-11, 2009

In addition, some on-going work has been submitted to different conferences/workshops:

• G. Popa, E. Gourdin, F. Legendre, and M. Karaliopoulos, "On Maximizing Collaboration in Wireless Mesh Networks Without Monetary Incentives", RAWNET 2010 Resource Allocation in Wireless Networks (with WiOpt 2010), Avignon, France, 4 June 2010

• J. Lessmann, M. Schöller, F. Zdarsky, and A. Banchs, "Rope Ladder Routing: Position-Based Multipath Routing for Wireless Mesh Networks", 2nd IEEE WoWMoM Workshop on Hot Topics in Mesh Networking, Montreal, Canada, 10-17 June 2010

• P. Smith, A. Schaeffer-Filho, A. Ali, M. Schöller, N. Kheir, A. Mauthe, and D. Hutchison, "Strategies for Network Resilience: Capitalising on Policies", AIMS 2010, 21-25 June 2010, Zurich

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

Finally, in the framework of EC's events, flyers publicizing ResumeNet's activities have been distributed during the Future Internet Assembly which was held in Stockholm (Nov 23-24, 2009). Furthermore, the following presentation took place recently:

• A. Fischer, A. Berl, A. Galis, H. de Meer, "Network Virtualization in AutoI and ResumeNet, Future Internet Cluster Meeting, Sophia Antipolis, France, 9th March 2010

2.5.2. Further impact-making activities

University of Lancaster has new, significant links with two major Telcos:

- with BT, through a large new UK-India funded project in which Lancaster U. is leading the resilience activity and BT Research is leading the security work;
- with Telekom Malaysia (TM) through a new Lancaster-based PhD student who has worked for TM for the past 10 years, and will bring real-world information about resilience threats and also about relevant network topology/traffic information that may be useful to the research work within ResumeNet, initially for the remediation activities.

2.5.3. 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 first six months of 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	✓		Delivered before end of M7 to allow inclusion of the risk-assessment approach in the document.
1.2a	Defining metrics for resilient networking (Interim)	1	TUDelft	R	PU	M18	✓		Delivered on time
1.3a	Politics for resilience (Interim)	1	NEC	R	PU	M18	✓		Delivered on time
1.5a	First interim strategy document for resilient networking	1	ULANC	R	PU	M12	✓		Delivered with short delay
2.1a	First draft on defensive measures for resilient networks	2	FT	R	PU	M18	✓		Delivered with short delay
2.2a	First draft on new challenge detection approaches	2	ULg	R	PU	M18	✓		Delivered with short delay

2.3a	First draft on the remediation, recovery, and measurement framework	2	ULANC	R	PU	M18	✓		Delivered with short delay
3.1a	Taxonomy of P2P, Overlays and Virtualization techniques with respect to service resilience	3	UP	1	PU	M12	✓		Delivered with short delay
4.1a	Federation Requirements (Interim)	4	ETHZ	R	PU	M6	✓		Light deliverable in response to the request for inputs from FIREWorks
4.1b	Federation requirements (Final)	4	ETHZ	R	PU	M18	✓		Delivered with short delay
5.1	ResumeNet website and Wiki pages	5	ETHZ	O	PU	M2	✓		Delivered in time
5.2a	Yearly report on dissemination activities	5	FT	R	PU	M12	✓		Delivered with short delay
6.1	Project Management Guidelines	6	ETHZ	R	PP	M2	✓		Delivered in time
6.2a	Links between research and experimentation (Interim)	6	ULANC	R	PU	M6	✓		Light deliverable in response to the request for inputs from FIREWorks
6.2b	Links between research and experimentation (Final)	6	ULANC	R	PU	M18	✓		Delivered with short delay
6.3	Report on technical work in WP2 and WP3 during first year	6	ETHZ	R	PU	M12	✓		Delivered with short delay

3.2. Milestones

Table 3.2 Milestones

Milestone no.	Milestone name	Work package no	Lead beneficiary	Delivery 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
M5.1	Website and Wiki pages set up and operational	WP5	ETHZ	M2	Yes	M2	

4. Project management

The basic concern of the management team for this third period 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 fulfill 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 some 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 "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 will be 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 these six months included:

• **Maintaining synchronization of the whole Consortium on the project activities.** Management issues, communication on 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. As a result 2 of the project deliverables were delivered within the official delivery time, 2 with a delay of 2 weeks and 2 (the "light" FIREWorks deliverables) with a delay of four weeks. There was no case in which the hard deadline of 45 days after the official deliverable delivery date was exceeded.

- **Organization of physical meetings.** To monitor and coordinate the overall project work and also for discussion and workshops within individual WPs, two plenary meetings took place during the past half year: the third plenary meeting in Munich, Germany, 7-9 October 2009, and the fourth plenary meeting in Delft, NL, 20-22 January 2010. Both plenary meetings were combined with separate meetings of the Project Technical Committee. The list of meetings scheduled for the rest of 2010 is given in Table 4.1.
- **Meeting with the Advisory Board.** The Munich project meeting was combined with a meeting with the project Advisory Board members. Three of them were physically present there (Prof. Jean-Claude Laprie, Dr. Rick Schlichting, and Prof. Ruediger Grimm). The fourth member (Prof. Jim Kurose) joined remotely for the full duration of the meeting. The Consortium obtained a range of excellent and supportive comments from the reviewers, who brought extensive experience and viewpoints to the resilience problem and promoted different considerations of research problems addressed in individual research tasks.

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

Meeting	Context (scope)	Date	Location / Host
5th Project plenary meeting	The tri-annual plenary project meeting	17-19 May 2010	Uppsala, Sweden (University of Uppsala)
6th Project plenary meeting	The tri-annual plenary project meeting + 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	Beginning of November 2010	Brussels, Belgium

Last but not least, the project management saw the addition of a new member, Dr. Regina Notz from the Euresearch team of ETH Zurich. Dr. Notz replaced Mrs. Hodel in the provision of administrative support to the management. She has been instrumental in preparation of deliverables, meetings and this project review report.

5. Explanation of the use of the resources

Omitted from this version of the deliverable.