HIDENETS

ghly DEpendable IP-based NETworks and Services

www.HIDENETS.aau.dk

HIDENETS

Highly Dependable IP-based Networks and Services

(FP6 STREP, Jan. 2006-Dec 2008)

”End-to-end resilience solutions for vehicular scenarios”

HIDENETS Partners

Overview

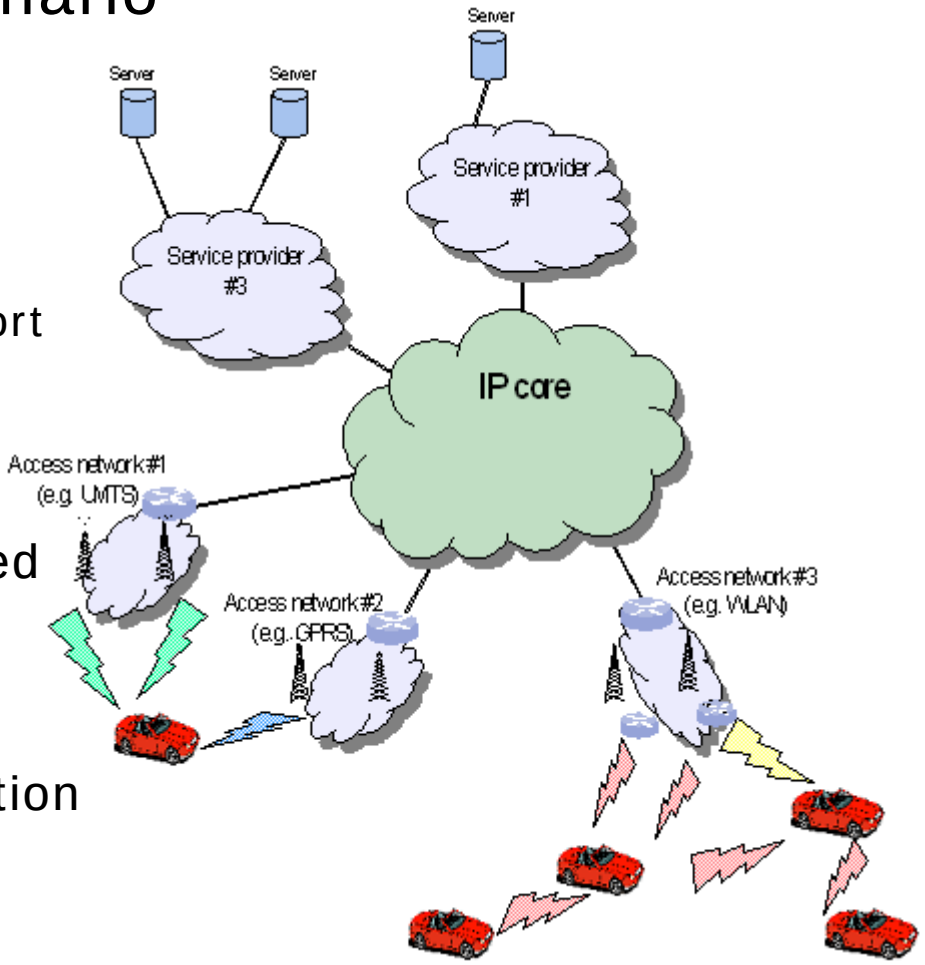
- The HIDENETS project: goals and challenges
- Resilient architecture and fault analysis
- Resilience mechanisms
- Evaluation of resilient systems
- Modelling, development, test of resilient solutions
- Test-beds for validation
- Dissemination and references
- Summary and outlook

HIDENETS Goals

- Develop and analyze **end-to-end resilience solutions**
  - for scalable distributed applications and mobility aware services
  - in ubiquitous communication scenarios
    - car2car communication with server-based infrastructure support
  - assuming highly dynamic, unreliable communication infrastructures
- **Overall goal**
  - The planned HIDENETS results will clearly show that solutions for new distributed applications with critical requirements on open communication infrastructures can be designed, implemented, and evaluated
- **Results**
  - Architectural solutions and resilience services (middleware and communication level)
  - Tools for design and testing during application development
  - Quantitative evaluation methodology and analysis results
  - Experimental proof-of-concept implementations

HIDENETS Network Scenario

- Infrastructure connectivity
  - IP-based core with heterogeneous access: Cellular, WLAN, etc.
  - Mobility (and QoS) support
  - Resilience through path redundancy/multi-homing
- Infrastructure services
  - Resilience via cluster-based architecture and/or distributed redundancy
- Ad-hoc domain
  - Resilience via communication protocols (L2-4) and HIDENETS middleware



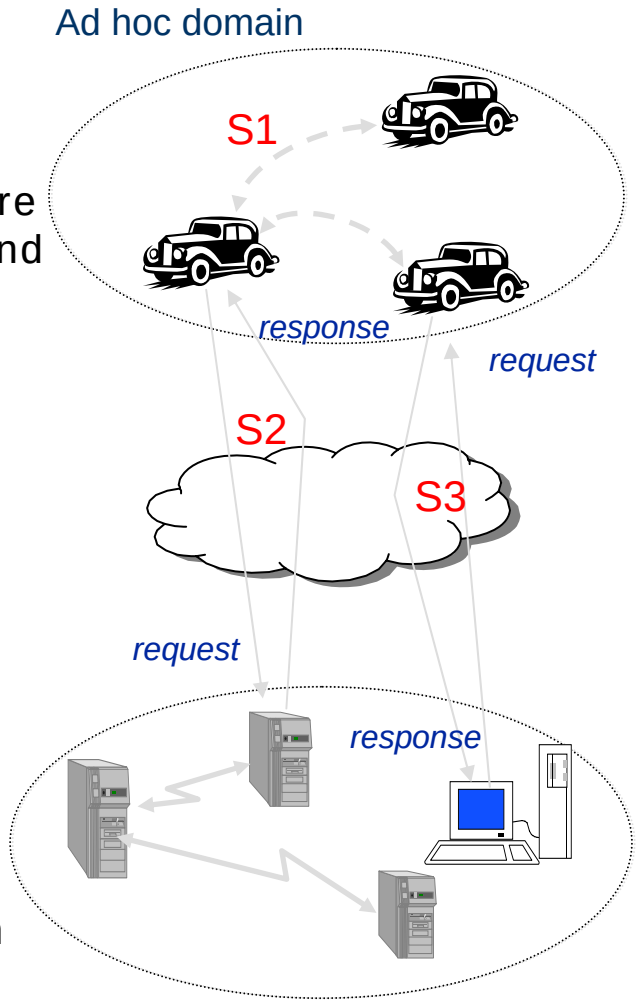
HIDENETS Challenges

- **Challenges** of the C2C/C2I scenarios
  - C2C = Car to car, C2I = Car to Infrastructure
  - Dynamicity/mobility: changing topologies and communication characteristics
  - Open systems with (C)OTS components
  - Heterogeneity: different network domains [and different node capabilities]
  - Resource limitations and strong cross-influence between system parts

  + large number of nodes…

- **Fault-categories**
  - **Design-time** and **run-time** faults
  - **Timing** (omission, crash) and value faults
  - **Transient** and **persistent** faults
  - **Accidential** and malicious causes

  Detailed fault models and consequences depend on application type and technical realization

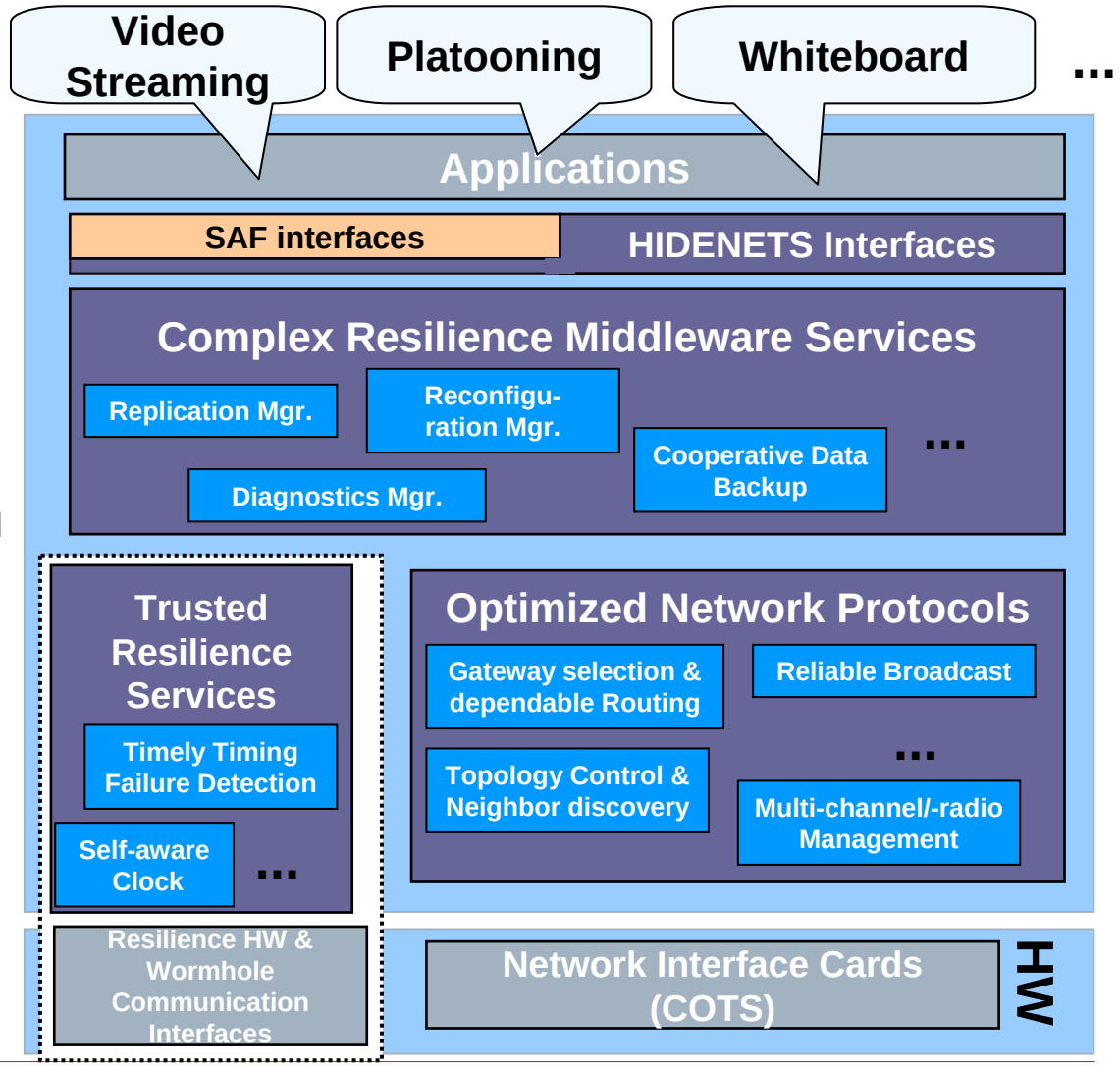


HIDENETS Resilience Architecture

- Resilience extends the classical notion of fault tolerance
  - level of adaptability, so as to be able to cope with system evolution and unanticipated conditions
- Resilience architecture provides functional view on HIDENETS resilience functions in compute or network nodes:
  - helps understand functional relationships
  - reflects relationship to SAForum (www.saforum.org) interface specification work
  - defines target architecture for evaluation topics and for resilience design and generation
  - serves to structure HIDENETS work items

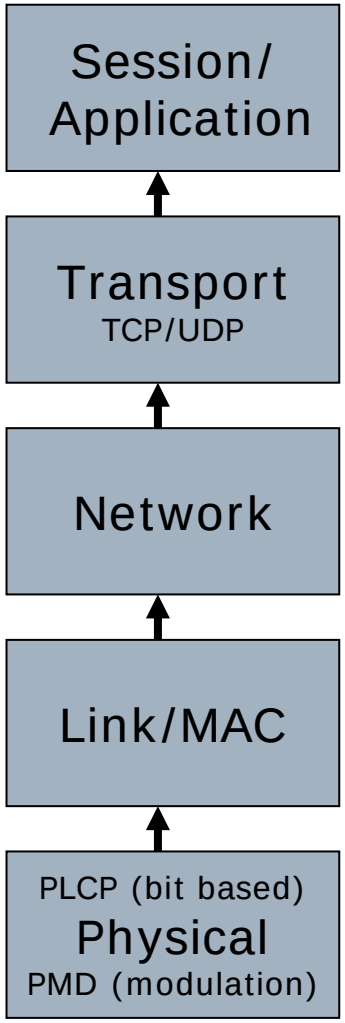
HIDENETS Resilience Architecture

- Resilience middleware and communication services
  - Remove burden from application developer → Cost efficiency
  - Dependability via careful specification and verification
- Hybrid architecture, 'trusted' part with
  - stricter timeliness properties
  - 'Critical' functions
  - Separate (physical/virtual) communication links



Fault Analysis

- **Idea: Improve the layered communication model in terms of enhanced resilience by analyzing possible faults, errors and failures and their consequences.**
- Identify relations between failures and resilience mechanisms based on a hierarchical communications model
- Focus on failures forwarded to the layer above (placed on the boundaries between the two layers)



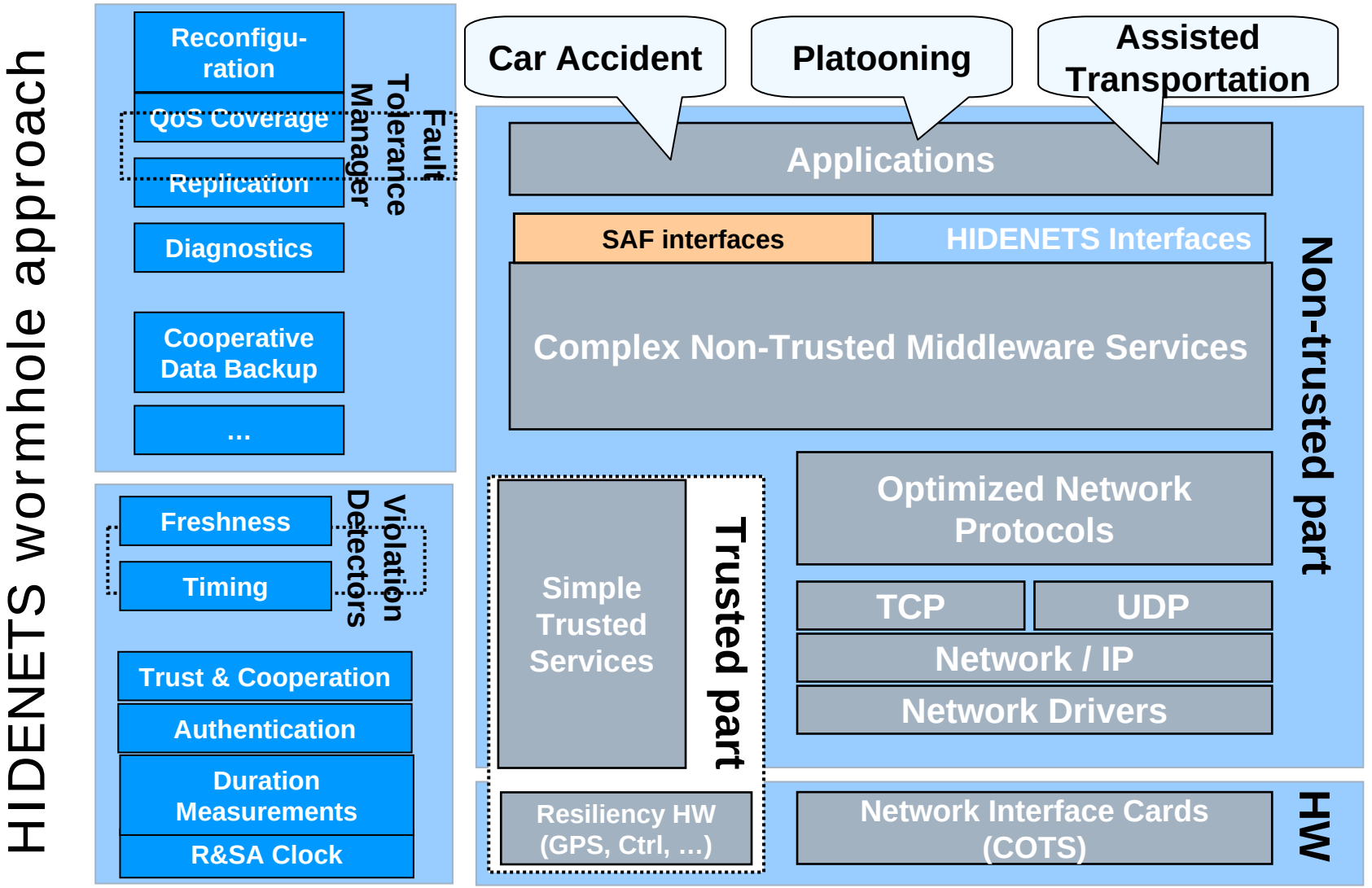
Resilience Services: Examples

- Multi-channel multi-radio architecture
  - Multi-channel MAC and Channel Assignment services
  - Allows for communication on nearby links in parallel by reducing/eliminating interference
  - Increases the capacity gain of Multi-Channel and allows for guaranteed connectivity
- IP resilient routing
  - Provides local fast reroute for proactive link state routing
  - Improves source-destination connectivity
- Reliable Broadcast
  - Based on hop-by-hop acknowledgments
  - Reduction of message forwarding and ACK events by local strategies based on circuit elimination → avoid broadcast storm problems

Resilience Services: Examples cont.

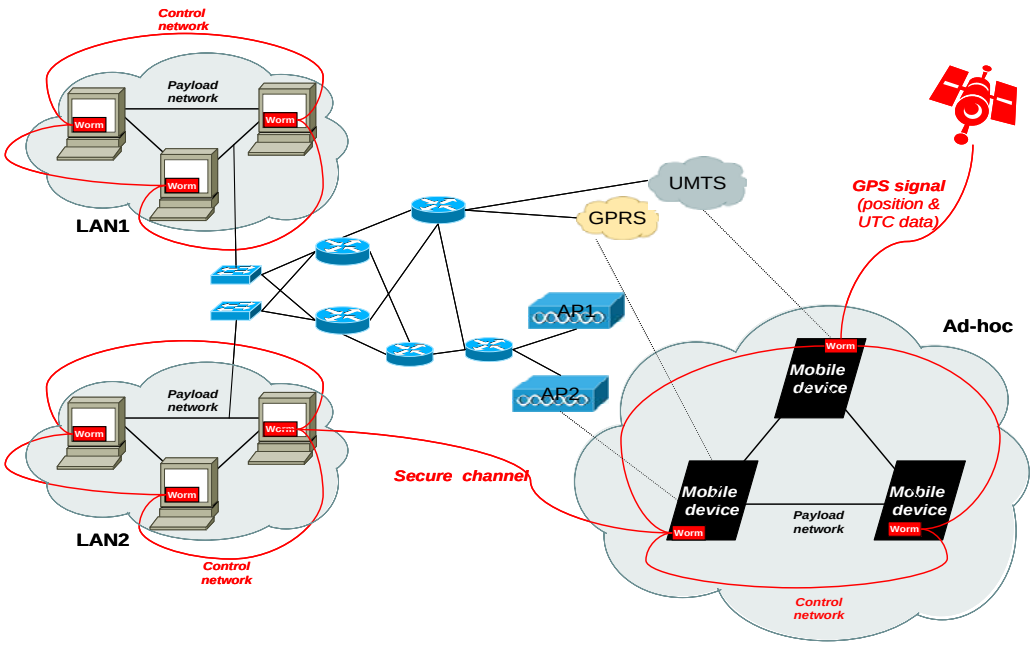
- Always Best Connected
  - Resilience in accessing infrastructure networks
  - Increased reliability by redundancy (using several access points), differentiation, and by smarter access point selection
- Replication Manager
  - Allows to implement replicated applications with dynamically changing state in the ad-hoc domain
  - Automatic selection of replica nodes based on node properties and communication quality
  - → increased application availability to clients
- Self-aware Clock
  - Provides clock value together with precision bounds wrt. global time
  - Derived e.g. from properties of synchronisation protocol

HIDENETS wormhole approach



Wormhole communication

- In ad-hoc domain
  - Dedicated interfaces and frequency channels (if available)
  - Less dynamic topologies, e.g. via increased transmission power
    - [→requires low traffic volumes]
- In infrastructure connectivity
  - Ideally also physically separated, but likely only logically in most cases

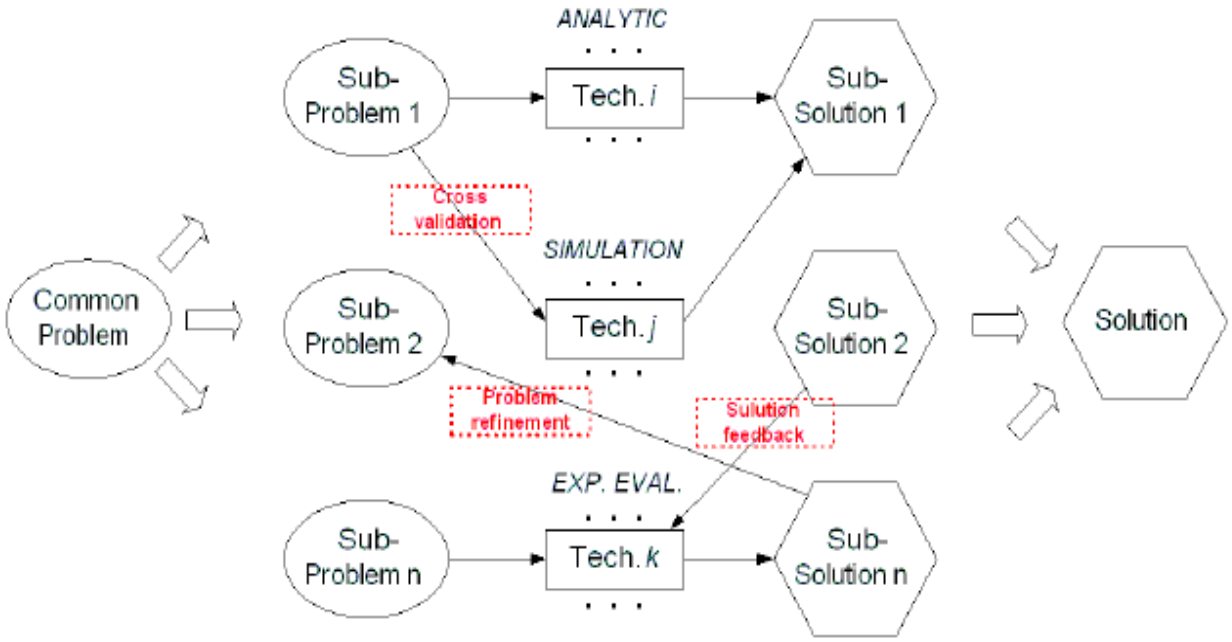


Quantitative Evaluation

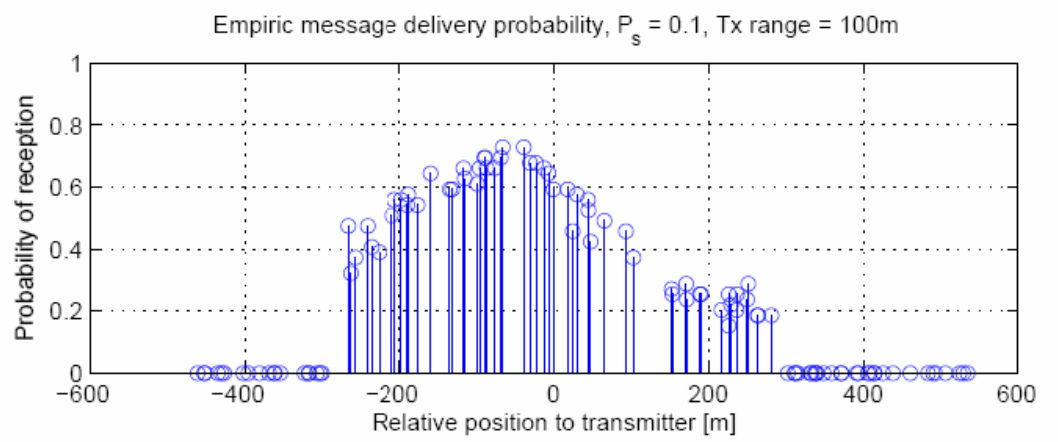
- Holistic approach aiming at end-to-end metrics, e.g.
  - Probability of successful execution of a series of user activities
- Combining different methodologies
  - Analytic Models: Numerical solutions of Markov /Petri-Net models, queueing models, integral expressions for connectivity metrics, ...
  - Simulations Models: NS2-based network simulations, Matlab based routing and broadcasting simulations, simulative solution methods for stochastic activity networks
  - Experimental measurements: using wireless communication as well as emulated dynamic topologies
- Three different evaluation types
  - Pointwise evaluation of HIDENETS services (in isolation)
  - Specific use-case driven analysis [details in last session]
  - Workflow for (semi-)automatic end-to-end analysis [details in last session]

A Holistic Approach to Quantitative Assessment

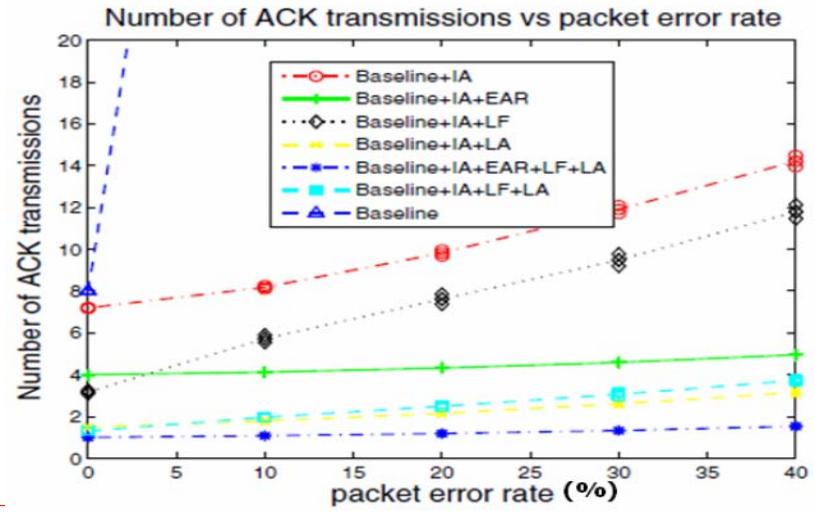
- A common problem consists of a set of sub-problems
- Each sub-model is solved using an appropriate solution technique
- The solution of the common problem is obtained by exploiting the interactions among different techniques



Point-Wise Evaluation: Broadcast Example



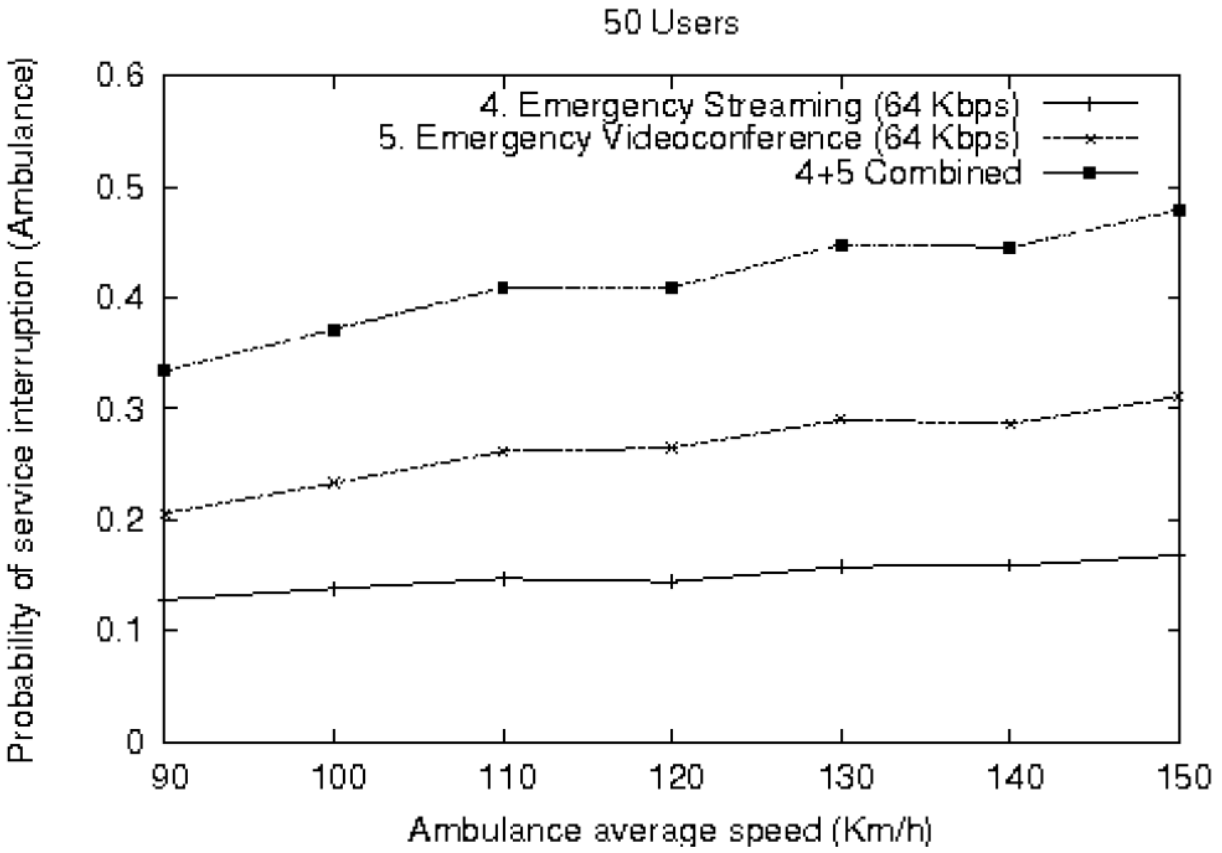
- NS-2 simulation of distance dependent reception probability



- Overhead in different reliable broadcast strategies

Use-Case Driven Analysis: Example

- Resulting dependability metric

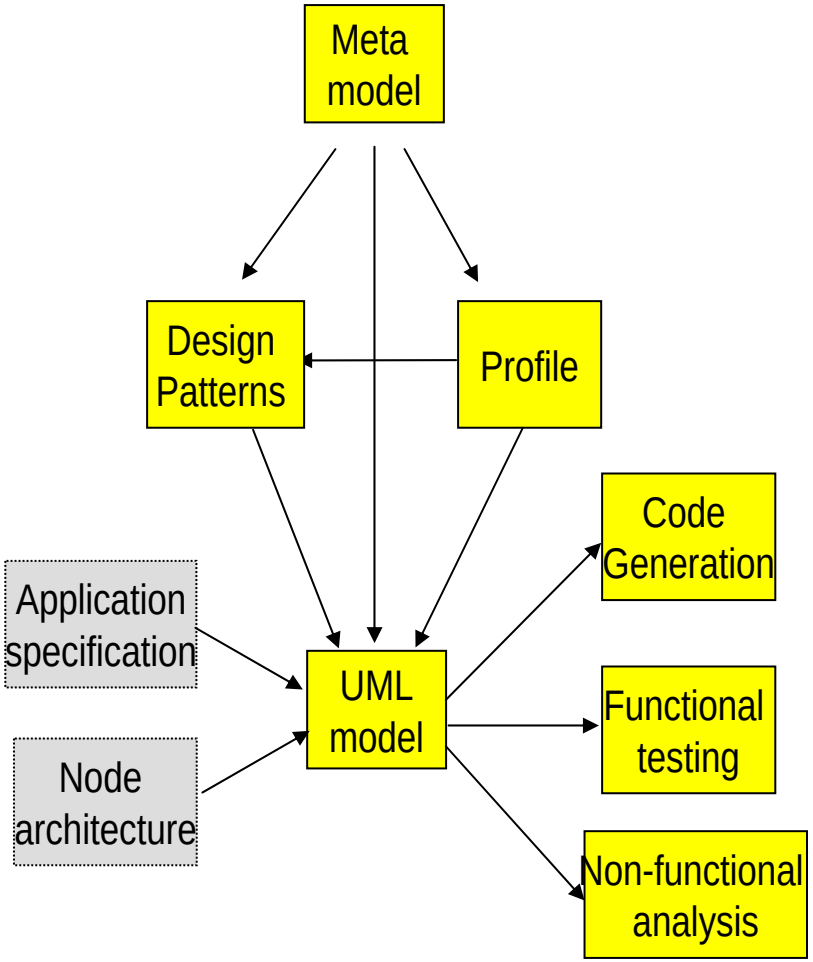


Main Evaluation Results

- Definition of methodologies for a holistic approach to the quantitative evaluation and analysis of the HIDENETS scenarios
- Evaluation and analysis of the HIDENETS resilient mechanisms and resilient communications mechanisms
- Holistic approach to evaluate the (user perceived) QoS provided by integrated HIDENETS scenarios

Design Methodology and Modelling Framework

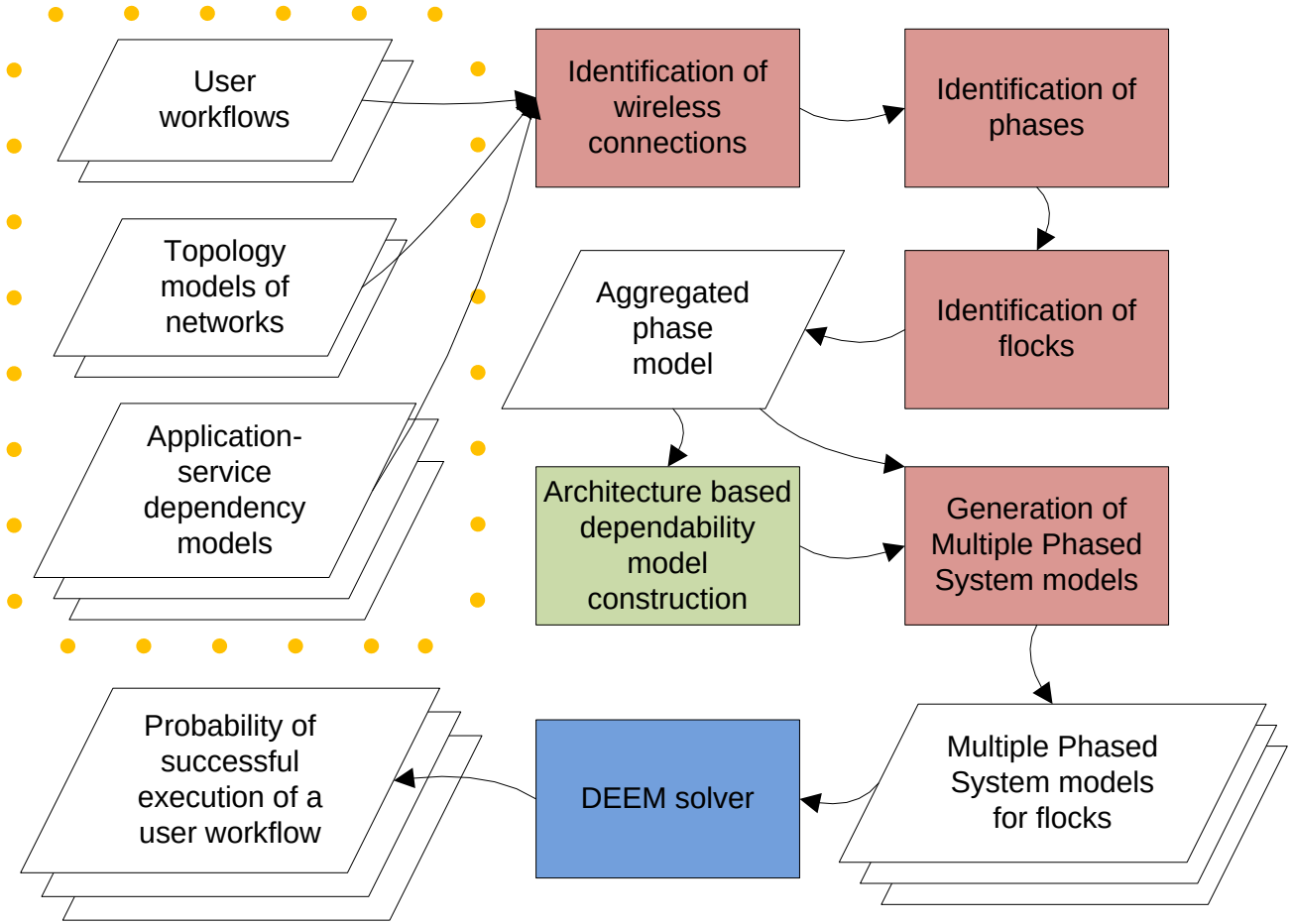
- Application development and analysis support
  - Meta-models
  - UML profiles
  - design patterns
- Elaboration of tool chain concepts
  - related model transformations and interfaces
- Testing framework
  - Determination of testing levels
  - Test selection problem
  - Testing Oracle



Modelling of Resilient Applications

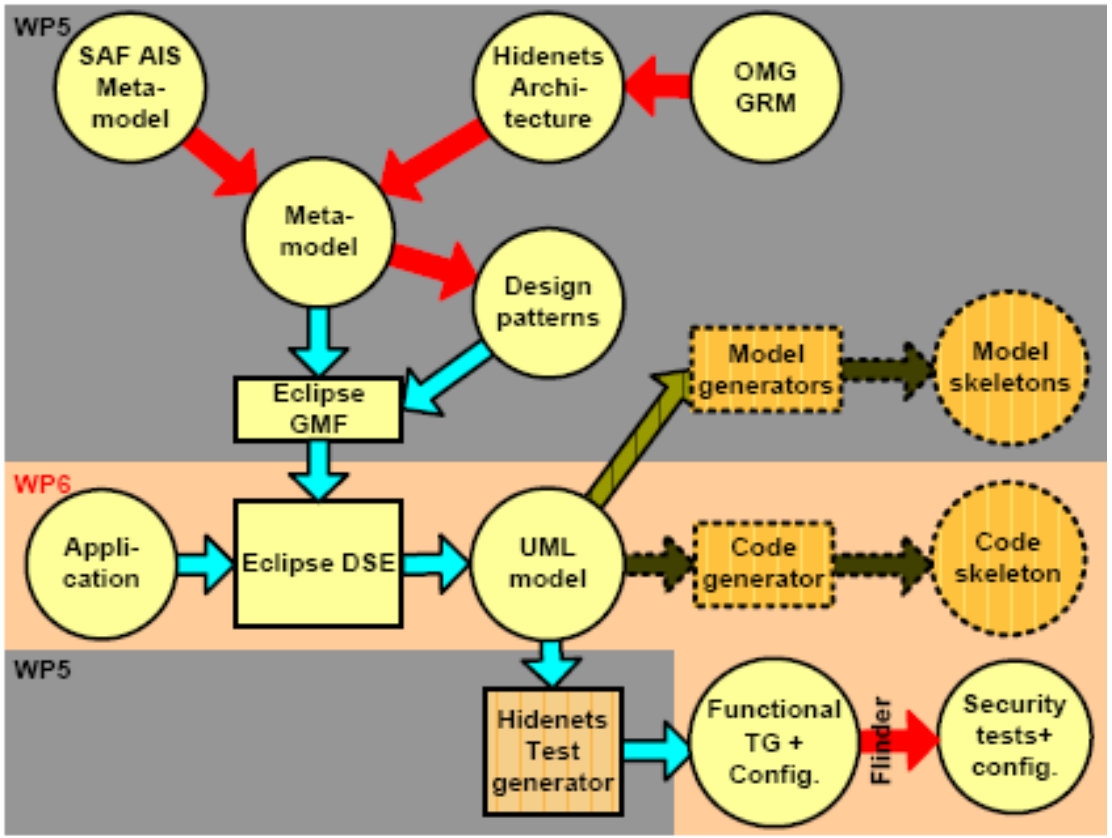
- Determining design context
  - Elaboration of tool-chain concepts
  - Research in related tools (Eclipse, model-transformations)
- Metamodel development
  - Elaboration of metamodel hierarchy levels
  - Definition of metamodel class stubs
  - Creation of UML profile stub
  - Study of applied UML profiles (SPT, SysML,...)
- Standards interaction
  - Eclipse, UML, SA Forum, Autosar

Semi-Automatic Evaluation Workflow



Concepts of HIDENETS Tool Chain

- **Meta-model**: synthesis of Hidenets architecture and SA Forum application interface spec.
- **Design patterns**: facilitate the application of best practices
- Meta-model and design patterns serve as input for creating the domain specific editor (DSE)

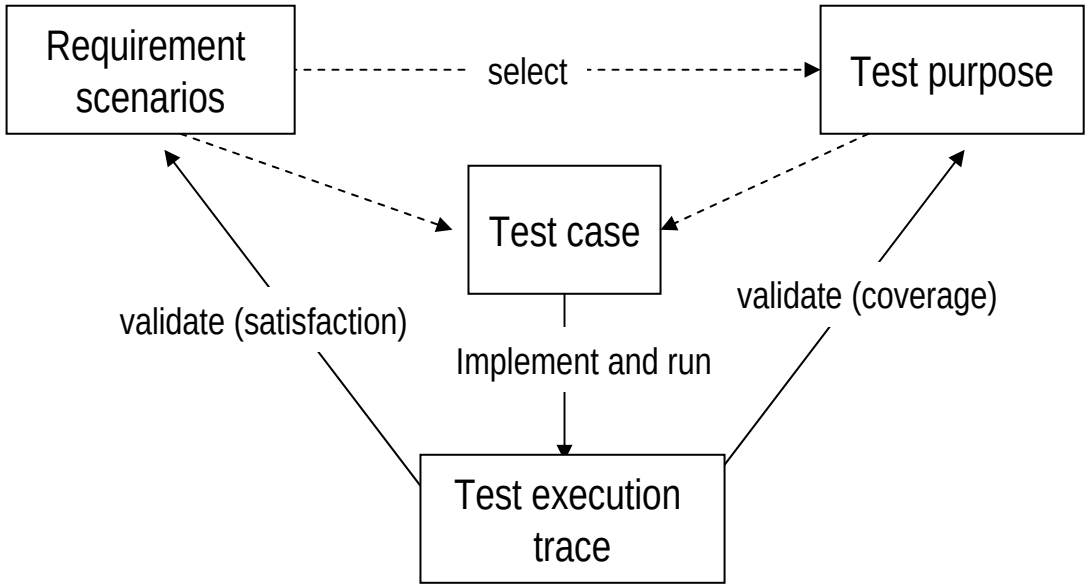


Testing of Hidenets Resilience Applications

- Test challenges in mobile environments
  - Highly dynamic scenarios
  - Need for a rich test environment
    - To control the delivery of messages based on location information, the communication delays (e.g. to stress the global ordering of messages), …
    - To account for sophisticated mobility models (to control the movement of nodes)
    - Include network and context simulators
- Verification case study
  - Mobile group membership protocol
  - Specification review, modelling, and testing
- Main achievements
  - Definition of a language that describes interaction scenarios in mobile settings
    - Extensions based on UML 2.0 Sequence Diagrams
  - Automated support to analyze and implement scenarios
    - graph matching algorithms to extract test scenarios from test traceS

Scenario-based Testing framework

- Requirements scenarios: capture key properties
- Test purposes: behavior covered by testing
- Test cases: interactions of test components and system under test, verdict assignment
- Test execution traces: actual, monitored traces



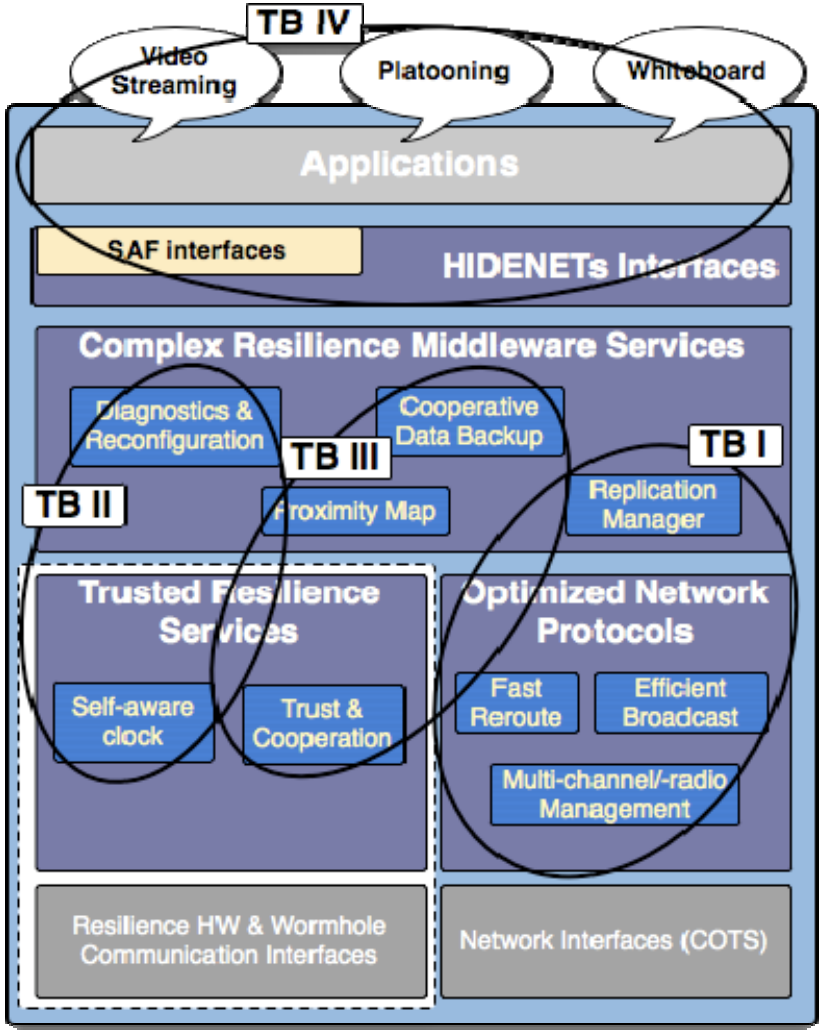
Test-Bed Based Validation – Motivation and Goals

- Test-beds were used for validating HIDENETS results

- Stand-alone benefit
- Focus on relevant HIDENETS functionality
- Parallel elaboration of node architecture
- Reduction of validation complexity
- Parallel development at multiple sites

Four Test-Beds

- Resilient communication
  - Communication enhancements in dynamic ad-hoc networks
- Platooning
  - Focusing on timeliness properties and hybrid architecture solutions
  - TORCS simulator for mobility emulation, real or emulated wireless communication
- Distributed Black Box
  - Opportunistic cooperative data backup
- Application development
  - Infrastructure based high-availability cluster solutions
  - Use of development tools



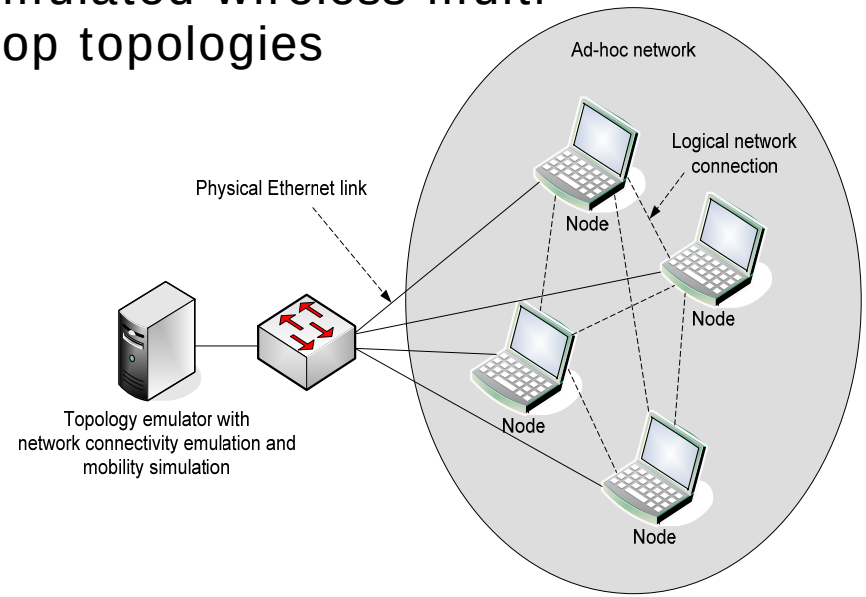
Test-Beds and their Scope

- A complex resilient application developed on top of the HIDENETS solutions using model-based development methods. It involves both the infrastructure and the ad-hoc domain. Moreover, it illustrates the feasibility of using HIDENETS concepts, methods and middleware for high availability applications, like SAForum [8]
- A Platooning application that is used as a proof-of-concept for the ability to detect and react to timing faults, to assure safety and to handle certain malicious intrusions.
- A distributed black-box application with the crucial middleware functionality that provides major dependability benefits in this application setting.
- Resilient communication protocols for ad-hoc (car to car) networks and their impact on higher layers.

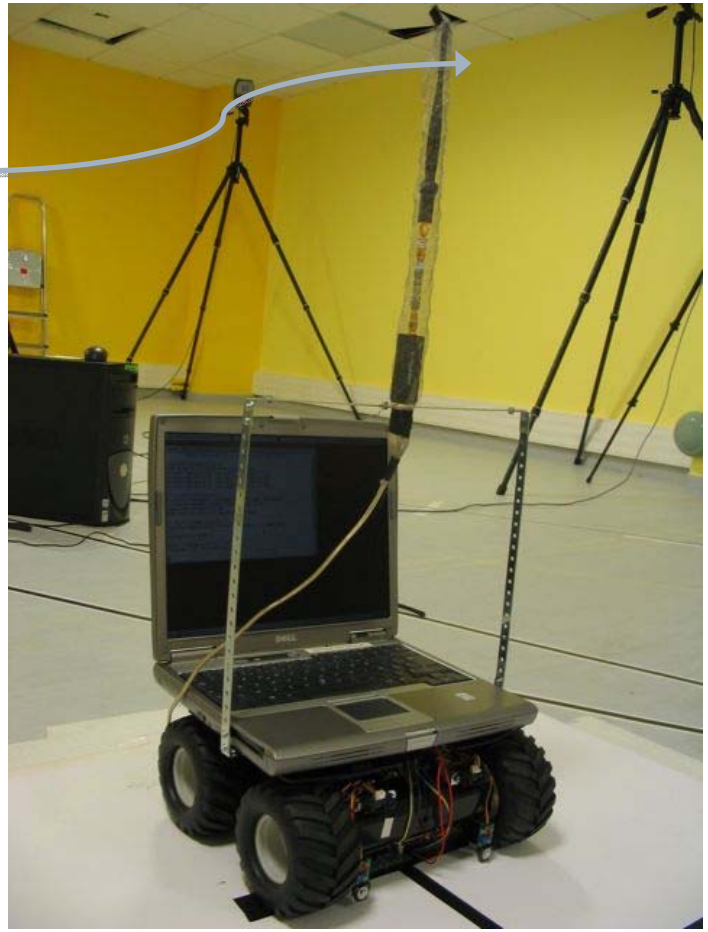
Test-Bed Approaches

Mobility and wireless communication

- 'scaled down' WLAN links and real node mobility; example: DBB test-bed
- emulated wireless multi-hop topologies



Attenuator



Dissemination Goals

- Transfer of HIDENETS concepts and results to industrial and governmental organisations and academic environment through
  - cooperation with standards groups
    - Service Availability Forum (SAForum)
    - Car to Car Communication Consortium
  - broad dissemination activities
    - dissemination pipeline, conference watchlist continuously updated
  - review of project progress for planning use of intellectual property
  - work with industry for transfer of HIDENETS results and know-how
- **Papers published in major conference proceedings, and journals, presentations: see the HIDENETS web page for details**

Open Challenges

- Medium-term (now – 2010)
  - Cost-effective development and runtime environments supporting dependability properties in the day-to-day IT industrial development and deployment process --> **sustainable growth in the European IT industry**
- Longer-term – (2010 – 2013)
  - Advancement in standardization process towards Seamless Integrated Resiliency and Security, to promote massive use of ICT for relevant business, governmental, private services

Relevant Web Pages

- www.HIDENETS.aau.dk
- www.saforum.org
- www.**car**-to-**car**.org
- http://cordis.europa.eu/
- http://ec.europa.eu/**information_society**

HIDENETS Resilience Solutions - Summary

- Resilience services
  - Middleware functions: service replication in ad-hoc domain, cooperative data storage, fault-detection and reconfiguration, intrusion-tolerant agreement, adaptivity
  - Architectural differentiation, wormhole environment: self-aware clock, timing failure detection
  - Enhanced communication protocols (L2-L4): multi-radio and multi-channel management, routing, (reliable) broadcast, cross-layer parameter adaptation, optimized infrastructure connectivity
- Application development support
  - Design patterns, meta models, domain-specific editors
  - Test specifications and verification approaches for mobile scenarios
- Quantitative Evaluation
  - Analytic models (Markovian, SAN), simulations (MATLAB, ns2), experimental
  - Point-wise evaluation of HIDENETS services
  - Application/Use-case specific end-to-end analysis
  - Workflow for semi-automatic dependability analysis
- Prototyping: Four test-beds

Technical deliverables are available on the HIDENETS web-page: www.hidenets.aau.dk