Mobility & Dependability

David Powell
LAAS-CNRS
Roadmap

- **Dependability**
- **Mobility**

- Concepts
- Recent research
- Ongoing and future research
Definition

(J.C. Laprie)

Dependability

Delivery of service that can justifiably be trusted, thus avoidance of failures that are unacceptably frequent or severe
The Dependability Tree

Dependability
- Means
  - Fault Prevention
  - Fault Tolerance
  - Fault Removal
  - Fault Forecasting
- Threats
  - Faults
  - Errors
  - Failures
- Attributes
  - Availability
  - Reliability
  - Safety
  - Confidentiality
  - Integrity
  - Maintainability
- Security
- Authorized actions

(J.C. Laprie)
The Dependability Tree

Threats
- Faults
- Errors
- Failures

& Mobility?
Mobility

Mobile devices...
- limited resources (weight, volume...)
- autonomous energy
- potentially hostile environment

...that communicate
- wirelessly

...and react
- depending on their context
Mobility

Mobile devices...
- limited resources (weight, volume...)
- autonomous energy
- potentially hostile environment

...that communicate
- wirelessly

...and react
- depending on their context

Accidental physical faults:
specific or aggravated
- energy exhaustion
- breakage, corrosion, pressure, temperature...
- noise, interference...
- ...
Mobility

Mobile devices...
- limited resources (weight, volume...)
- autonomous energy
- potentially hostile environment

...that communicate
- wirelessly

...and react
- depending on their context

Malicious attacks:
numerous vulnerabilities
- energy exhaustion
- theft, vandalism...
- physical substitution
- jamming
- eavesdropping
- interception
+ sensitive context data
- location
- ...

Adream
**Mobility**

Mobile devices...
- limited resources (weight, volume...)
- autonomous energy
- potentially hostile environment

...that communicate
- wirelessly

...and react
- depending on their context

**Development faults:**
all the difficulties of distributed systems
- concurrency
- non-determinism
- communication delays
- absence of common clock

+ specificities
- resource constraints
- neighborhood broadcast
- dynamic connectivity
- context-dependency
The Dependability Tree

Threats
  - Faults
  - Errors
  - Failures

& Mobility?

more, or more likely: need dependability!
The Dependability Tree

Means
- Fault Prevention
- Fault Tolerance
- Fault Removal
- Fault Forecasting

& Mobility?
Dependability Means

Fault Prevention ➤ Prevent occurrence or introduction of faults

Fault Tolerance ➤ Avoid service failures in the presence of faults

Fault Removal ➤ Reduce number and severity of faults

Fault Forecasting ➤ Estimate number, incidence and likely consequences of faults
Roadmap

Dependability

Fault Tolerance
  cooperative backup

Fault Removal
  testing

Fault Forecasting
  experimental evaluation
  model-based evaluation

Mobility

ongoing and future research
Fault Tolerance

cooperative backup

Fault Removal
testing

Fault Forecasting
experimental evaluation

model-based evaluation

ongoing and future research
Fault Tolerance in Mobile Setting

Distributed *non-mobile* fault-tolerance

- replicate data and/or processes on different nodes to survive node failures and/or attacks
  - replicated data, e.g., weighted voting [Gifford 1979]
  - replicated processes, e.g., Delta-4 [Powell 1991]
  - byzantine FT in WANs, e.g., Zyzzyva [Kotla *et al* 2007]
  - P2P systems, e.g., FT DHT's [Naor & Weider 2003]

**What does mobility bring?**

- disconnections and partitioning

new issues depending on frequency and granularity
Node churn model
Partitionable system model
Sparse-connectivity model
Sparse-connectivity model + intermittent access to fixed infrastructure
Cooperative Backup

Motivation
- long-range wireless connectivity is expensive
- mobile data production increasing at higher rate than long-range wireless bandwidth
- free short-range P2P communication (Wi-Fi, Bluetooth)
- leverage computing device ubiquity

Key ideas
- continuous backup as a background operation
- adapted to intermittent connectivity scenarios
  - *intermediate backup* on neighboring devices
  - *final backup* on reliable Internet store
- assumes user credentials survive data/device loss or failure
Cooperative backup challenges

- **Availability of intermediate backups**
  - (n,k)-erasure coded redundant backups

- **Security and performance of intermediate backups**
  - small blocks of compressed data (and meta-data)
  - single instance storage + convergent block encryption + Merkle hash-tree with signed root

- **Cooperation security**
  - accountable but self-identified participants (SUCV's)
  - Sybils discouraged through reputation scheme that rewards long-term use of same identifier
Fault Tolerance
   cooperative backup

Fault Removal
   testing

Fault Forecasting
   experimental evaluation

model-based evaluation

ongoing and future research
Testing in Mobile Setting

What does "integration" and "system" testing mean when the "units" move?
- depends on application and properties to be verified

What modelling technique is appropriate for describing mobile systems, and their tests?
- graphical scenario languages

How should the specificities of mobile systems be included in the modelling technique?
- dynamic system topology
- broadcast communication towards unknown neighboring nodes
- context dependencies
Scenario-Based Testing

- **Requirement scenario**: fragment of behavior, capturing key properties
- **Test purpose scenario**: an interaction pattern to be covered
- **Test case**: interaction of test components and SUT, verdict assignment
- **Test execution traces**: actual, monitored traces, which can be checked to see whether they:
  a) satisfy a given requirement scenario
  b) cover a given test purpose
Scenario-Based Testing

Graphical scenario language:
- UML sequence diagrams
- plus mobility extensions:
  - neighborhood broadcast
  - system topology
  - topology changes

Requirement scenario ➠ select ➤ Test case ➤ Test execution trace ➤ Test purpose scenarios

validate (satisfaction) ➤ implement and run ➤ validate (coverage)
GMP Test Purpose Example

Spatial View

Event View

n1:GMP    n2:GMP    n3:GMP

Changement de configuration de C1 à C2

hello (Safe, RangeNotSafe)

hello from n2

par

SPGetLeader

SPGroupChange

par

SPGetLeader

SPGroupChange
Passive Testing Environment

- **SUT** (Execution support)
- **Network simulator**
- **Context simulator**

**Trace of communication events**

**Requirement scenario**

**Test purpose**

**Graph sequence matching**

**GraphSeq tool**

**Mobility model**

**Trace of successive node topologies**

- **C1**
- **C2**
- ...
Roadmap

Fault Tolerance
- cooperative
- backup

Fault Removal
- testing

Fault Forecasting
- experimental evaluation
- model-based evaluation

Dependability

Mobility

ongoing and future research
Experimental Evaluation in Mobile Setting

Simulated mobile system
- ☀ cheap
- ☀ repeatable
- ☹ abstraction of reality
- ☹ boring

Real mobile system
- ☹ very expensive
- ☹ quasi-unrepeatable
- ☀ reality
- ☀ exciting
Experimental Evaluation in Mobile Setting

Simulated mobile system:
- 🎁 cheap
- 🎁 repeatable
- 😞 abstraction of reality
- 😞 boring

Real mobile system:
- 😞 very expensive
- 😞 quasi-unrepeatable
- 😁 reality
- 😁 exciting

Scaled model of mobile system:
- 🎁 within reach of funding agencies
- 🎁 quasi-repeatable
- 😁 real hardware/software environment
- 😞 scaling inaccuracies
- 😁 great fun!
# Scaled Mobility Platform

<table>
<thead>
<tr>
<th>Feature</th>
<th>Real system</th>
<th>Scaled model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless communication range</td>
<td>WiFi</td>
<td>100 m</td>
</tr>
<tr>
<td>Position-awareness accuracy</td>
<td>GPS</td>
<td>5 m</td>
</tr>
<tr>
<td>Node size</td>
<td>Road vehicles</td>
<td>a few meters</td>
</tr>
<tr>
<td>Node speed</td>
<td>tens of km / hour</td>
<td>a few decimeters</td>
</tr>
</tbody>
</table>
Mobility Representation

- Physical tracks
  - itinerary + event-triggering waypoints drawn on floor using tape
A Real Experiment

Scaled implementation of a distributed black-box application (EU Hidenets project)

- critical data backed-up cooperatively between vehicles
- can be queried should an accident occur
Mobility Representation

- **Physical tracks**
  - itinerary + event-triggering waypoints drawn on floor using tape

- **Virtual tracks**
  - software-implemented itinerary and velocity profiles using positioning service
A Real Experiment

Scaled implementation of a distributed black-box application (EU Hidenets project)

- critical data backed-up cooperatively between vehicles
- can be queried should accident occur

Observations

- testing with real wireless network
  - more asynchronous than expected (alternation between stable and unstable periods)
  - uniform disk assumption for communication range is, as expected, far from reality

- testing in real mobile hardware/software environment
  - convincing proof-of-concept prototype
  - but small number of nodes
Fault Tolerance
- cooperative backup

Fault Removal
- testing

Fault Forecasting
- experimental evaluation
- model-based evaluation

ongoing and future research
Model-based Evaluation in Mobile Setting

Behavior model(s)

- failure rates
- repair rates
- coverages
- ...

Dependability measure(s)

$R(\lambda t)$

Mobility model

Adream
Dependability of Cooperative Backup

- Does cooperative backup increase dependability?
- What erasure coding parameters \((n,k)\) give the best results?
- How does mobility affect achievable dependability?
Time between encounters

1/\alpha
Time between connections

\[ \frac{1}{\beta} \]
Dependability of Cooperative Backup

Back-up process model
- \((n,k)\) erasure code: up to \(n\) fragments sent to contributors
- data safe \(\Rightarrow\) original data or \(k\) fragments have reached Internet store
- data lost \(\Rightarrow\) data owner and contributors failed before \(k\) fragments reached Internet store

Device failure model
- crash failures
- stochastic process
- exponential distribution (rate \(\lambda\))

Device mobility model
- stochastic processes
- exponential distributions
  - encounters with other devices (rate \(\alpha\))
  - connections to Internet (rate \(\beta\))
MF (mobile fragments)

SF (safe fragments)

OU (owner up)

OD (owner down)

DL (data lost)

DS (data safe)

m(MF) + m(SF) < k

m(SF) ≥ k

m(MF).β' contributor meets infrastructure

m(MF).λ' contributor fails

FC (fragments to create)

α owner meets contributor

n

m(MF).

owner fails

owner meets infrastructure

Adream
LRF vs. basic parameters

\[(n,k) = (3,2)\]

- \(\alpha\): device encounter rate
- \(\beta\): internet connection rate
- \(\lambda\): device failure rate

Data loss probability decreased by up to \(\alpha/\beta\)

Cooperative approach beneficial when:
- \(\beta/\lambda > 2\)
- \(\alpha/\beta > 10\)

Cooperative backup approach useless when \(\alpha/\beta < 1\)

- Loss reduction factor \(LRF\)
- Participant effectiveness \((\beta/\lambda)\)
- Connectivity ratio \((\alpha/\beta)\)
Ongoing & Future Work Directions

**Fault-tolerance**
- Mobility-explicit computing models and algorithmic building blocks: geo-registers, mobile consensus…
- Application case studies: on-demand car-pooling

**Testing**
- Simulation-based platform for controlled execution of context-aware requirement scenarios
- Automated verification of test execution traces w.r.t. requirement scenarios

**Experimental evaluation**
- Position-awareness technologies: UWB, Hagisonic StarGazer
- Fault-injection in mobile location-aware setting
- Scale-model platform for controlled execution of context-aware requirement scenarios

**Model-based evaluation**
- Model-based evaluation of cooperative automobile applications
- Stochastic mobility models based on experimentally-observed mobility patterns