Adream

Architectures dynamiques
reconfigurables pour
systèmes embarqués
autonomes mobiles

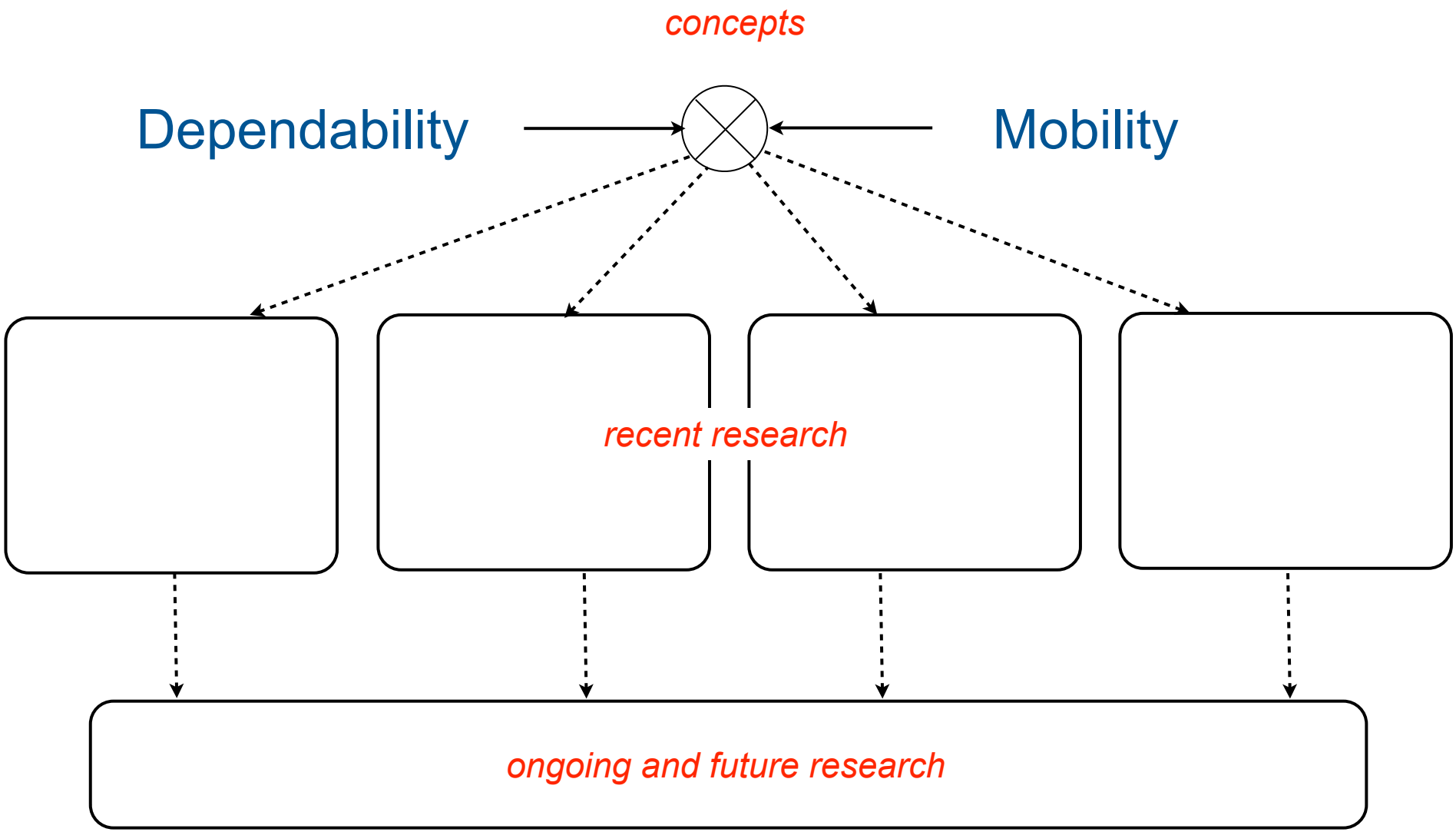
15 juin 2010

Mobility & Dependability

David Powell

LAAS-CNRS

Roadmap


concepts
Dependability
Mobility
recent research
ongoing and future research

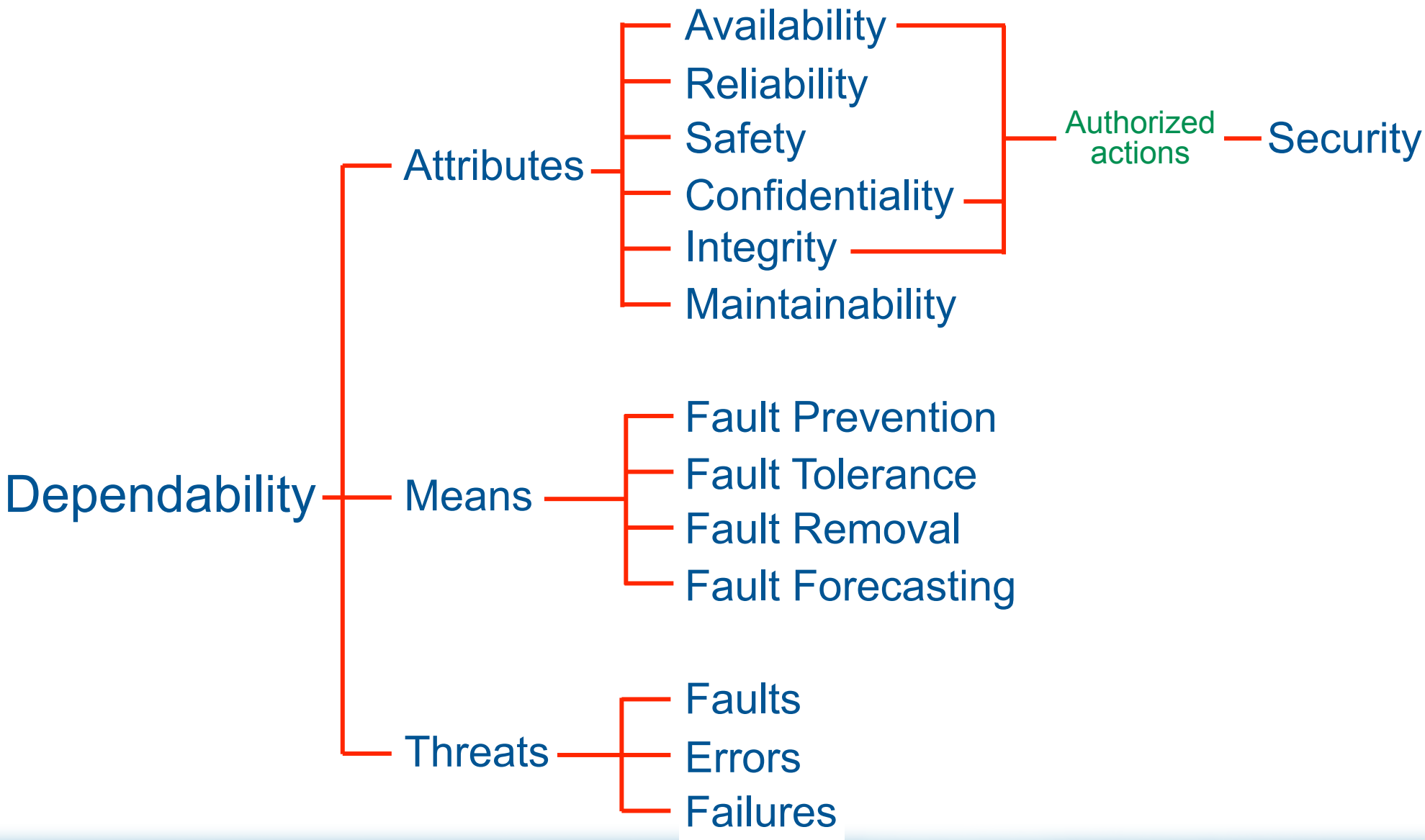
Definition

(J.C. Laprie)

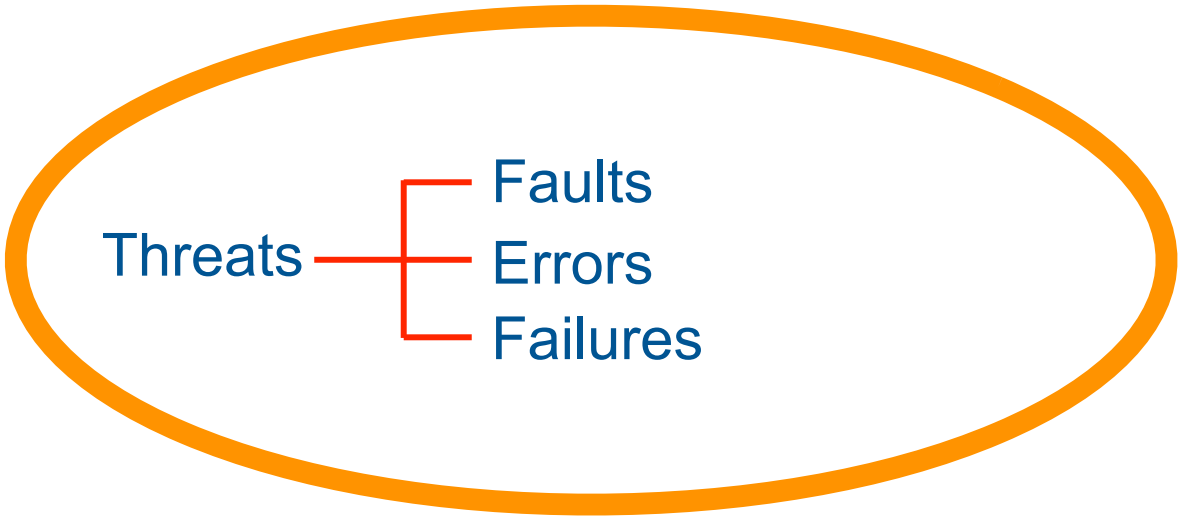
Dependability

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

The Dependability Tree (J.C. Laprie)



The Dependability Tree



& Mobility ?

Mobility

- **Mobile devices...**
  - limited resources (weight, volume...)
  - autonomous energy
  - potentially hostile environment
- **...that communicate**
  - wirelessly
- **...and react**
  - depending on their context

Mobility → *Accidental physical faults*:

- **Mobile devices...**
  - limited resources (weight, volume...)
  - autonomous energy
  - potentially hostile environment
- **...that communicate**
  - wirelessly
- **...and react**
  - depending on their context

specific or aggravated

- energy exhaustion
- breakage, corrosion, pressure, temperature...
- noise, interference...
- ...

Mobility → *Malicious attacks:*

- **Mobile devices...**
  - limited resources (weight, volume...)
  - autonomous energy
  - potentially hostile environment
- **...that communicate**
  - wirelessly
- **...and react**
  - depending on their context

numerous vulnerabilities

- energy exhaustion
- theft, vandalism...
- physical substitution
- jamming
- eavesdropping
- interception

+ **sensitive context data**

- location
- ...

Mobility → *Development faults:*

- **Mobile devices...**
  - limited resources (weight, volume...)
  - autonomous energy
  - potentially hostile environment
- **...that communicate**
  - wirelessly
- **...and react**
  - depending on their context

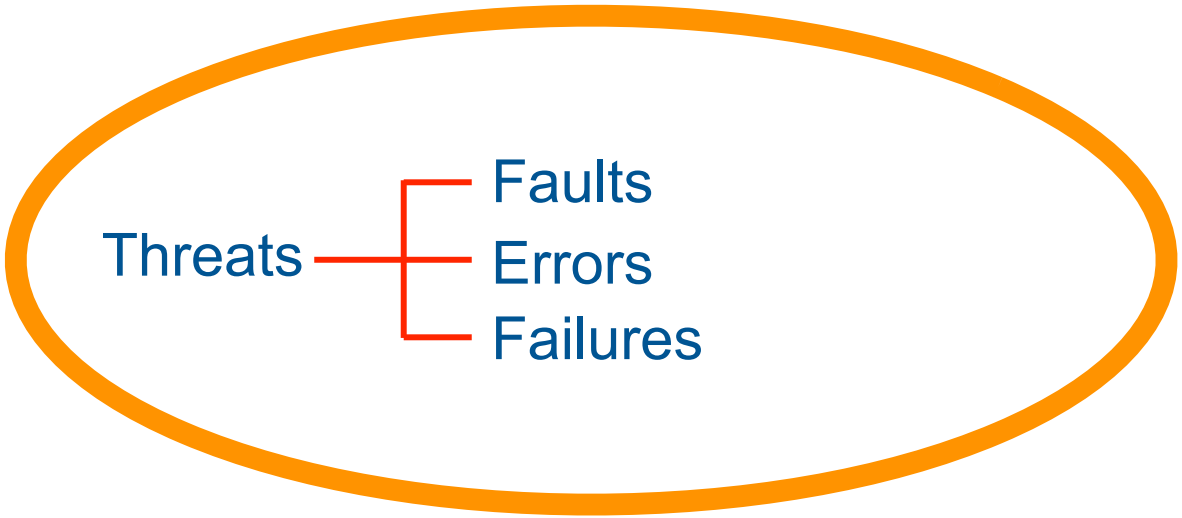
all the difficulties of distributed systems

- concurrency
- non-determinism
- communication delays
- absence of common clock

+ **specificities**

- resource constraints
- neighborhood broadcast
- dynamic connectivity
- context-dependency

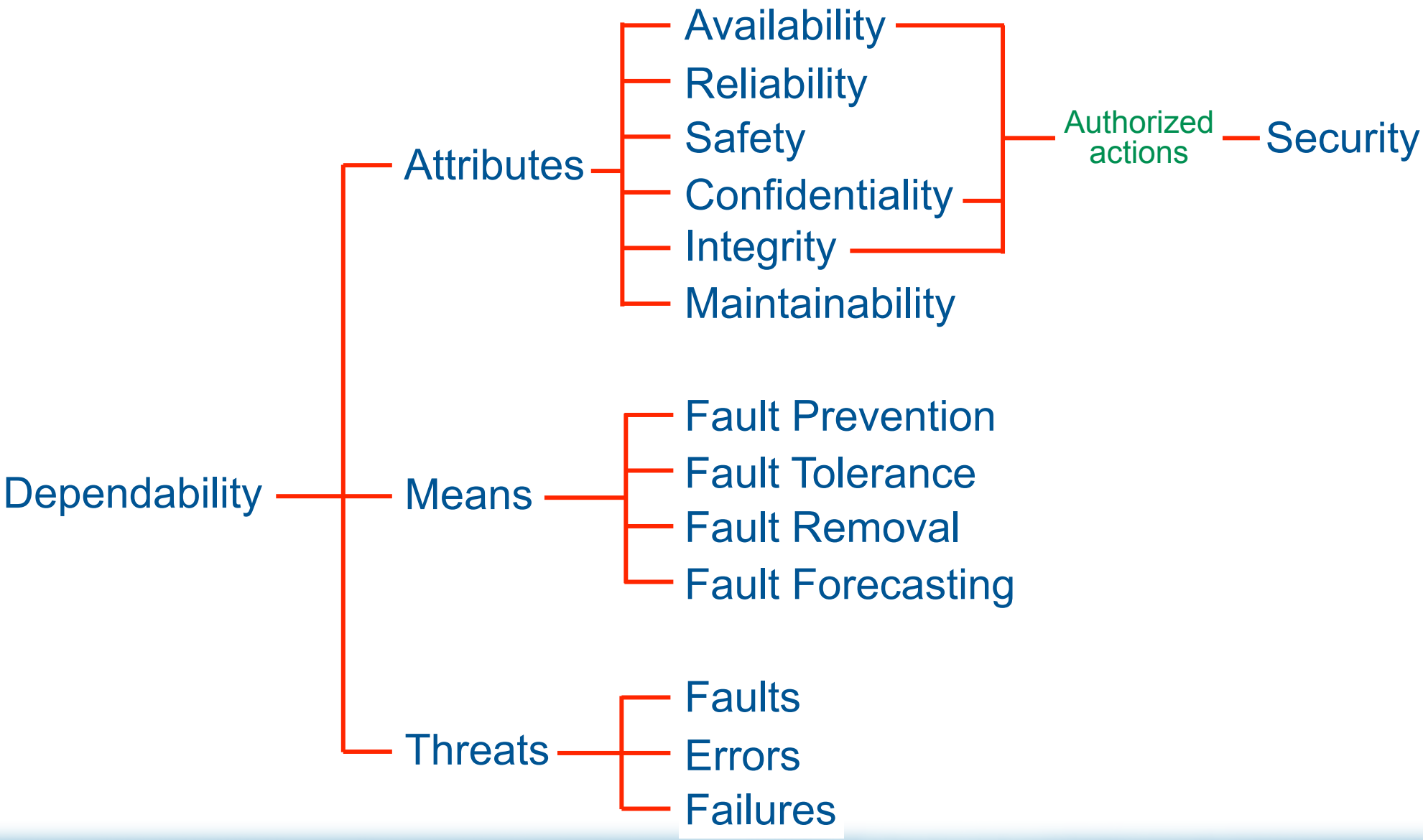
The Dependability Tree



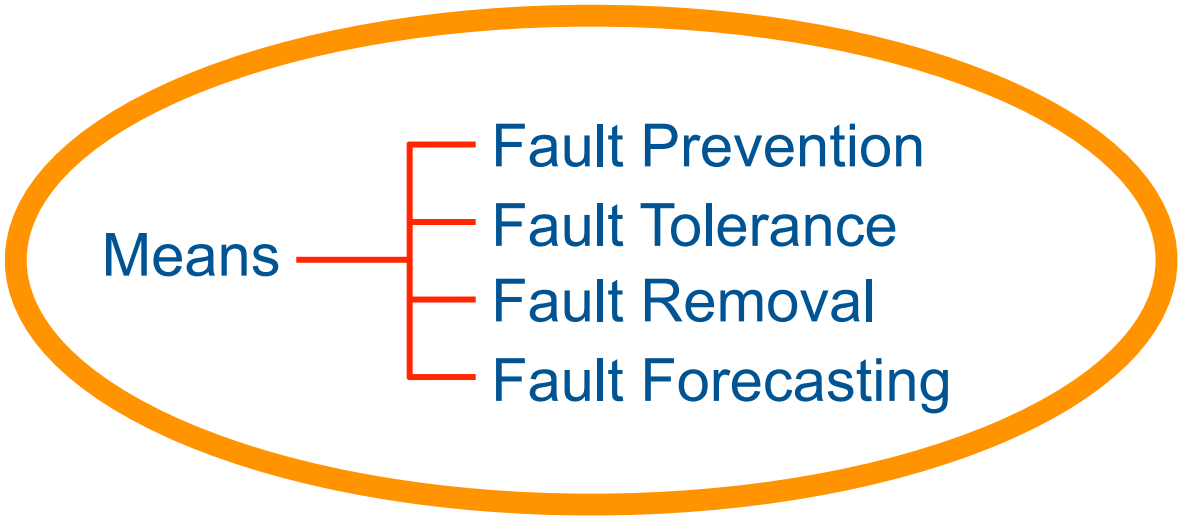
& Mobility ?

→ more, or more likely: need dependability!

The Dependability Tree



The Dependability Tree



& Mobility ?

Dependability Means

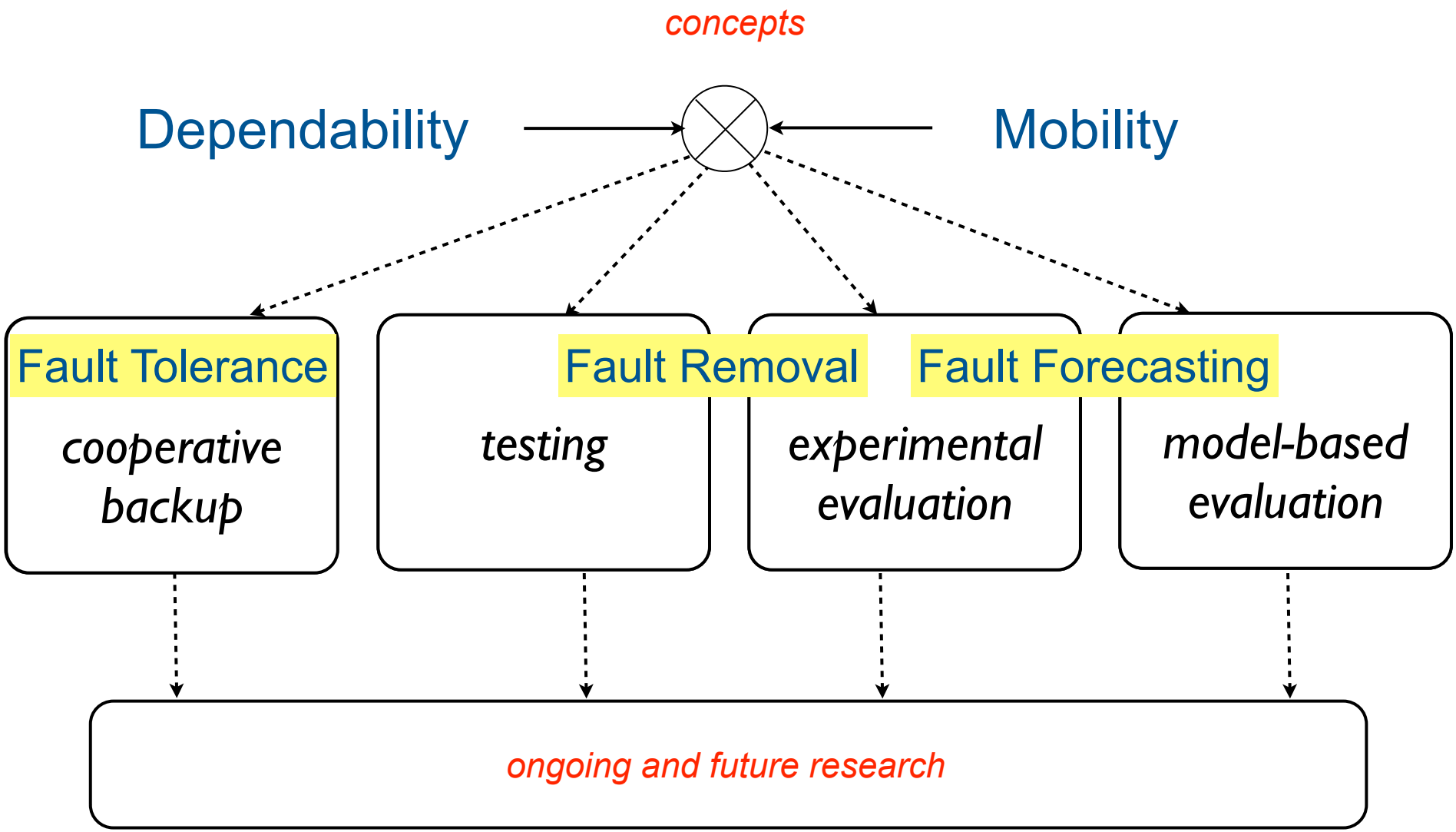
Fault Prevention ➠ Prevent occurrence or introduction of faults

Fault Tolerance ➠ Avoid service failures in the presence of faults

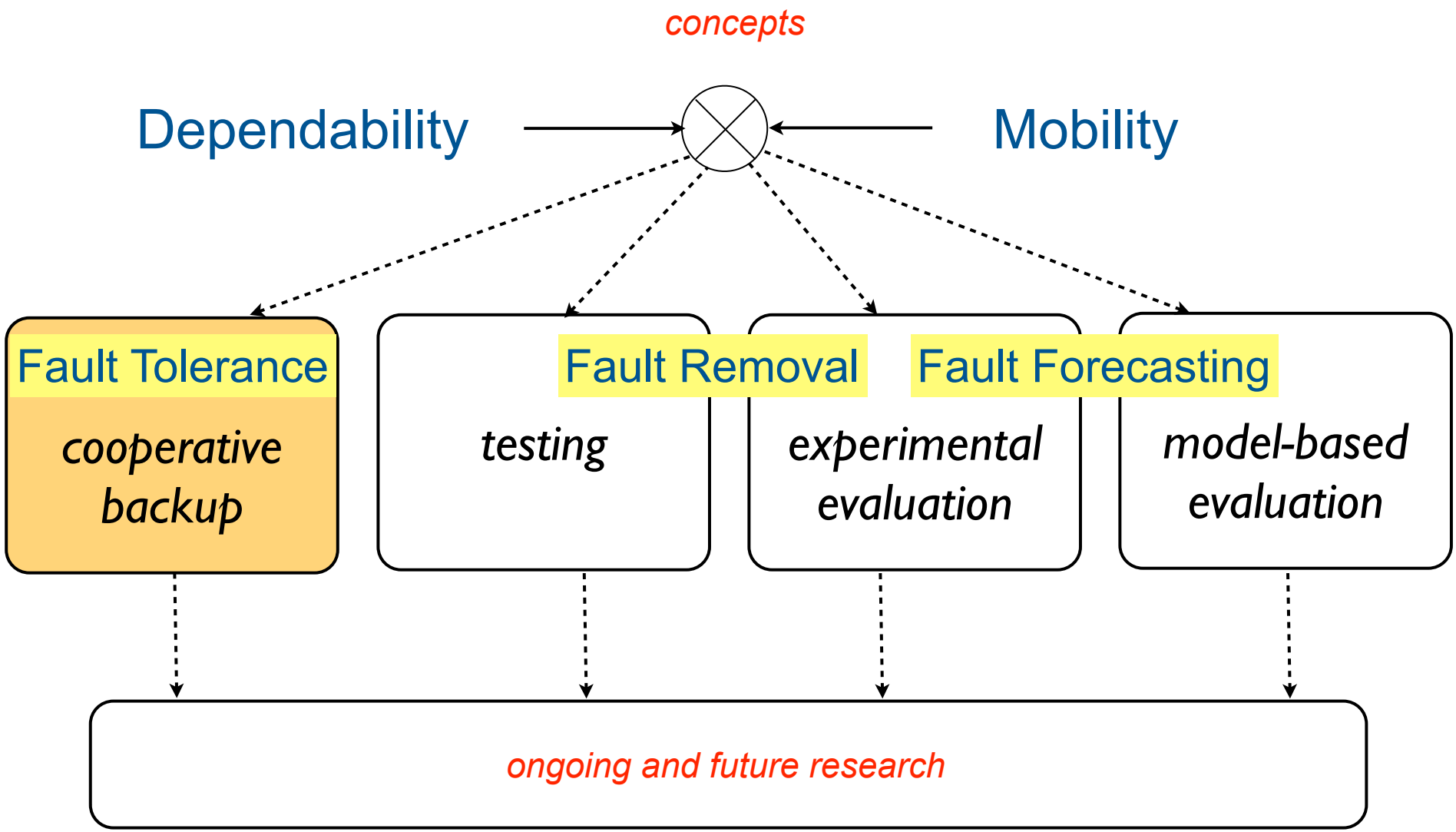
Fault Removal ➠ Reduce number and severity of faults

Fault Forecasting ➠ Estimate number, incidence and likely consequences of faults

Roadmap


concepts
Dependability
Mobility
Fault Tolerance
cooperative backup
Fault Removal
testing
Fault Forecasting
experimental evaluation
model-based evaluation
ongoing and future research

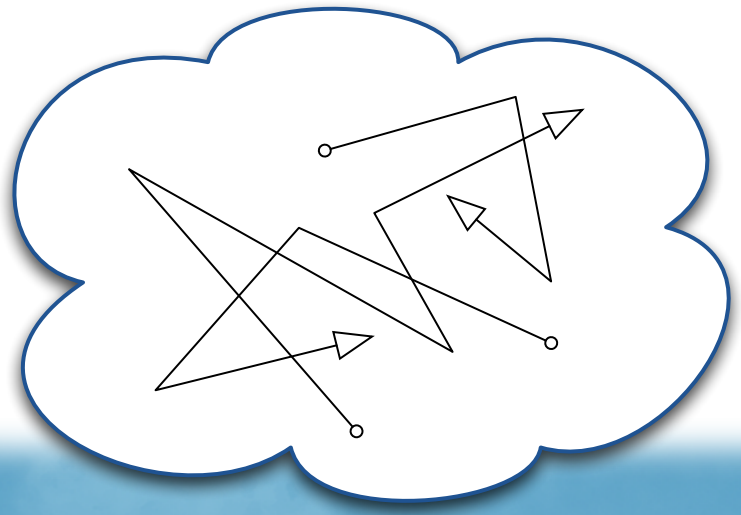
Roadmap

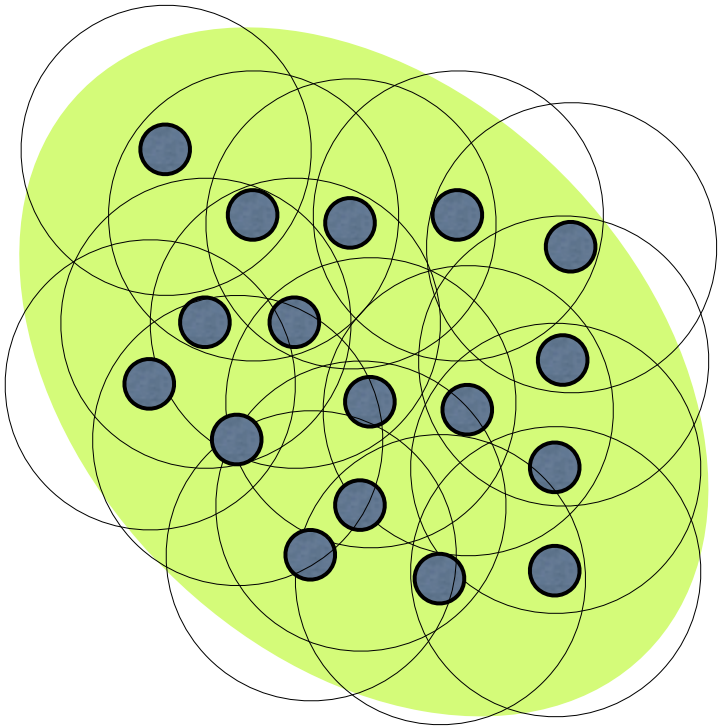

concepts
Dependability
Mobility
Fault Tolerance
cooperative backup
Fault Removal
testing
Fault Forecasting
experimental evaluation
model-based evaluation
ongoing and future research

Fault Tolerance in Mobile Setting

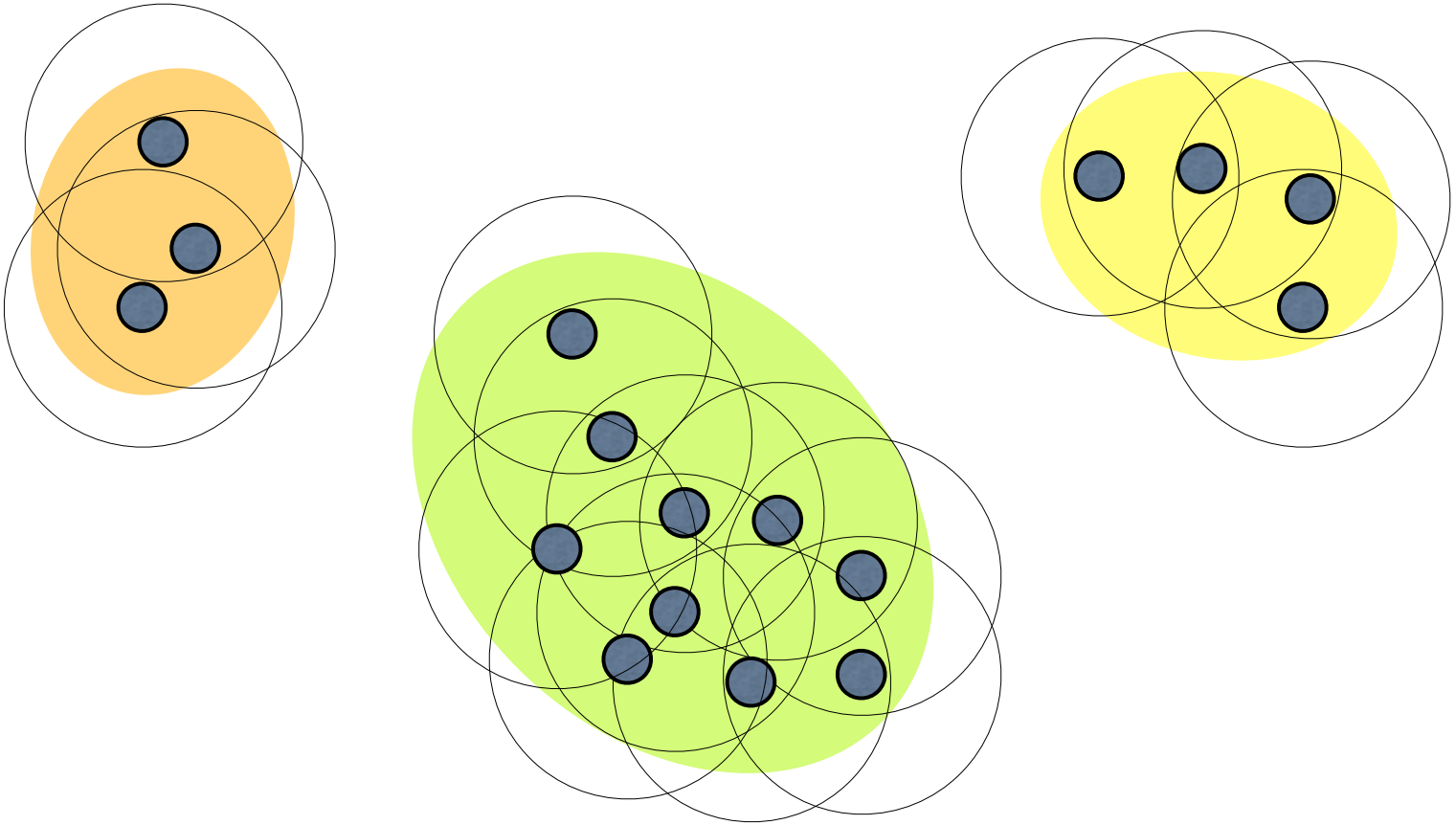
- **Distributed *non-mobile* fault-tolerance**
  - replicate data and/or processes on different nodes to survive node failures and/or attacks
    - replicated data, e.g., weighted voting [Gifford 1979]
    - replicated processes, e.g., Delta-4 [Powell 1991]
    - byzantine FT in WANs, e.g., Zyzzyva [Kotla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

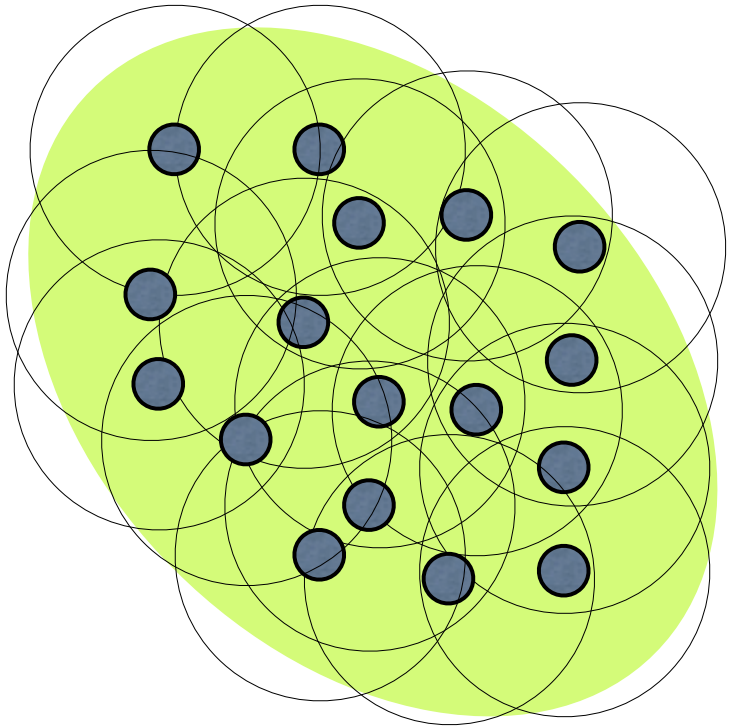
→ new issues depending on frequency and granularity

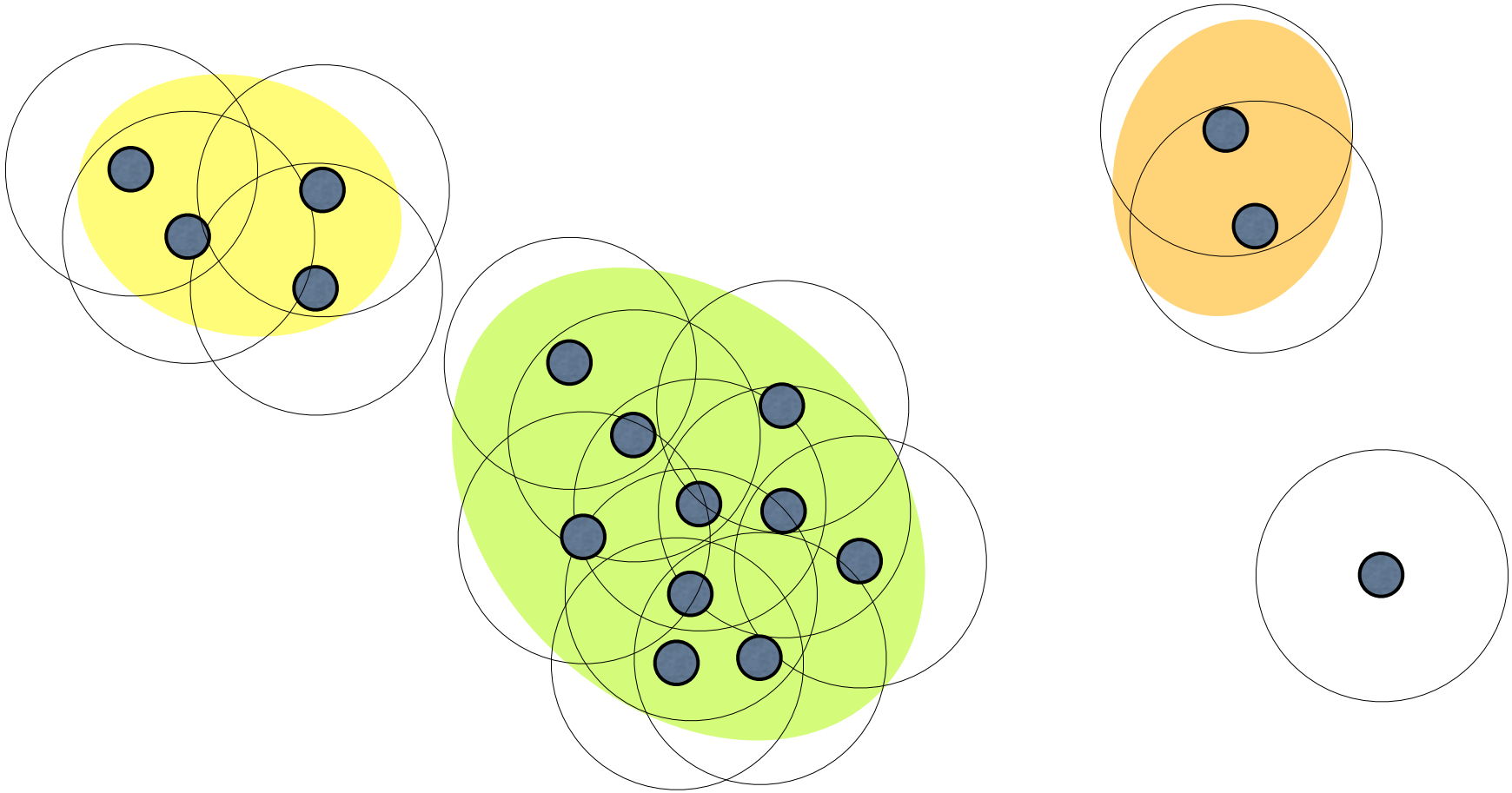




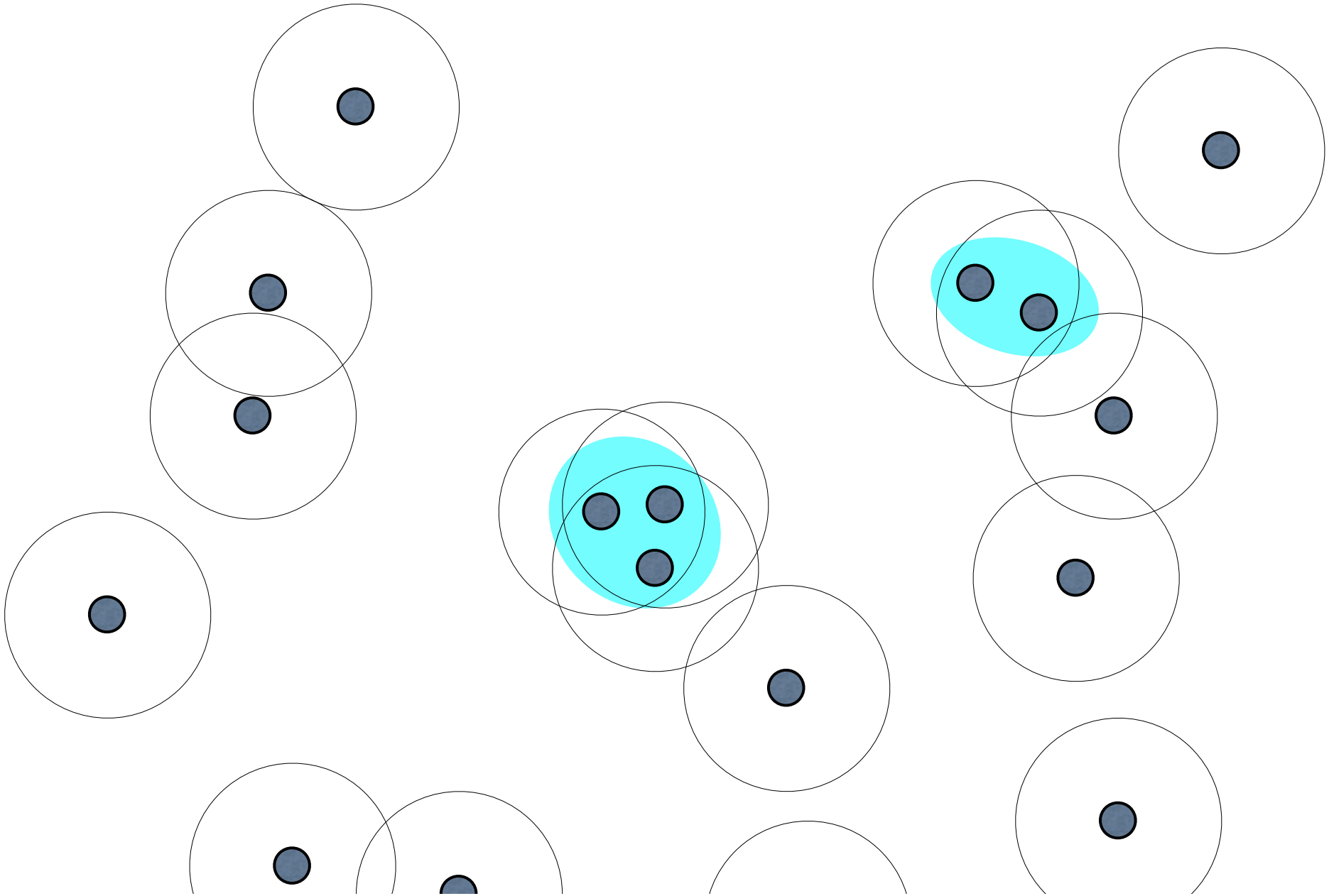
Node churn model



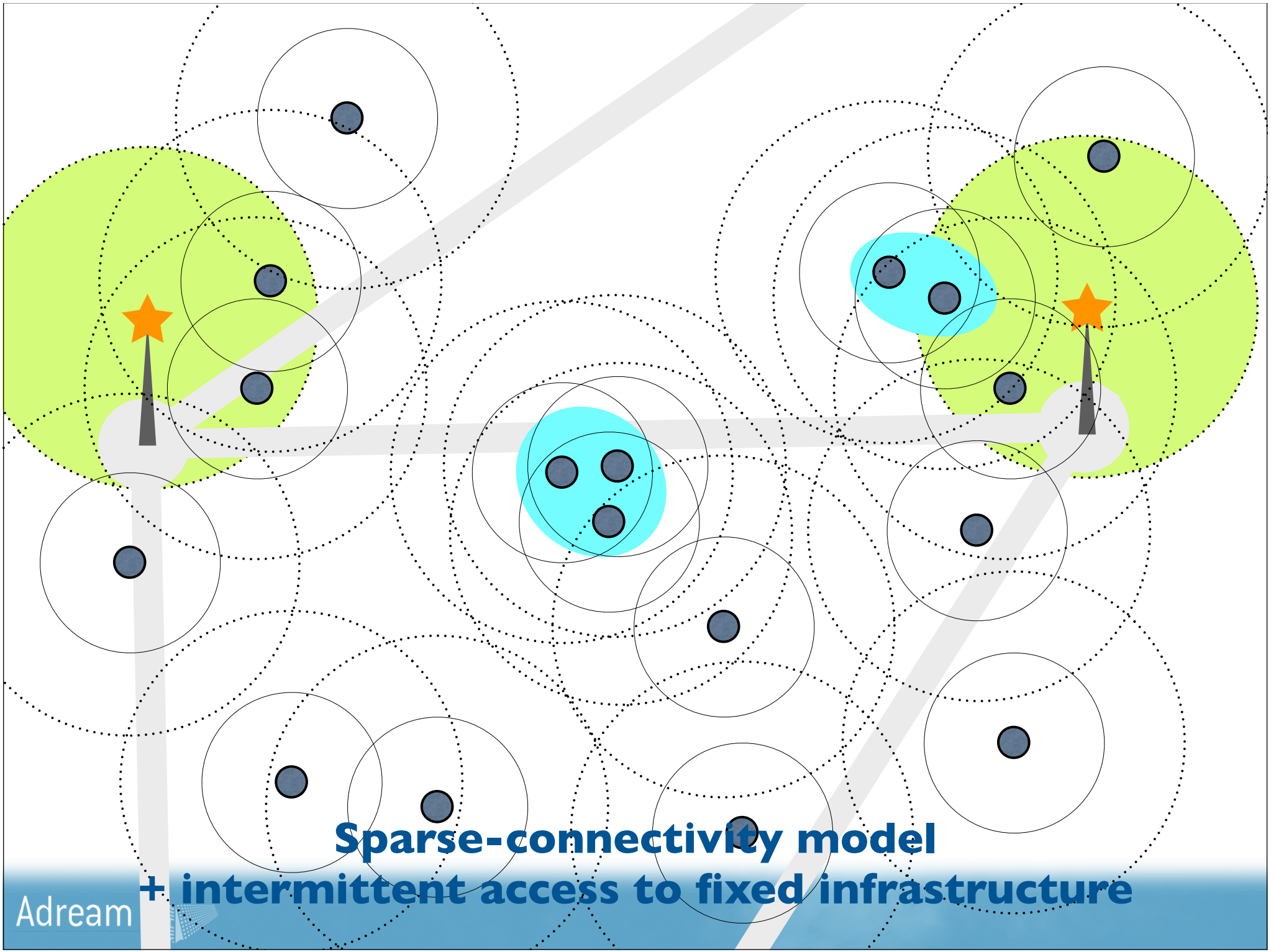




Partitionable system model

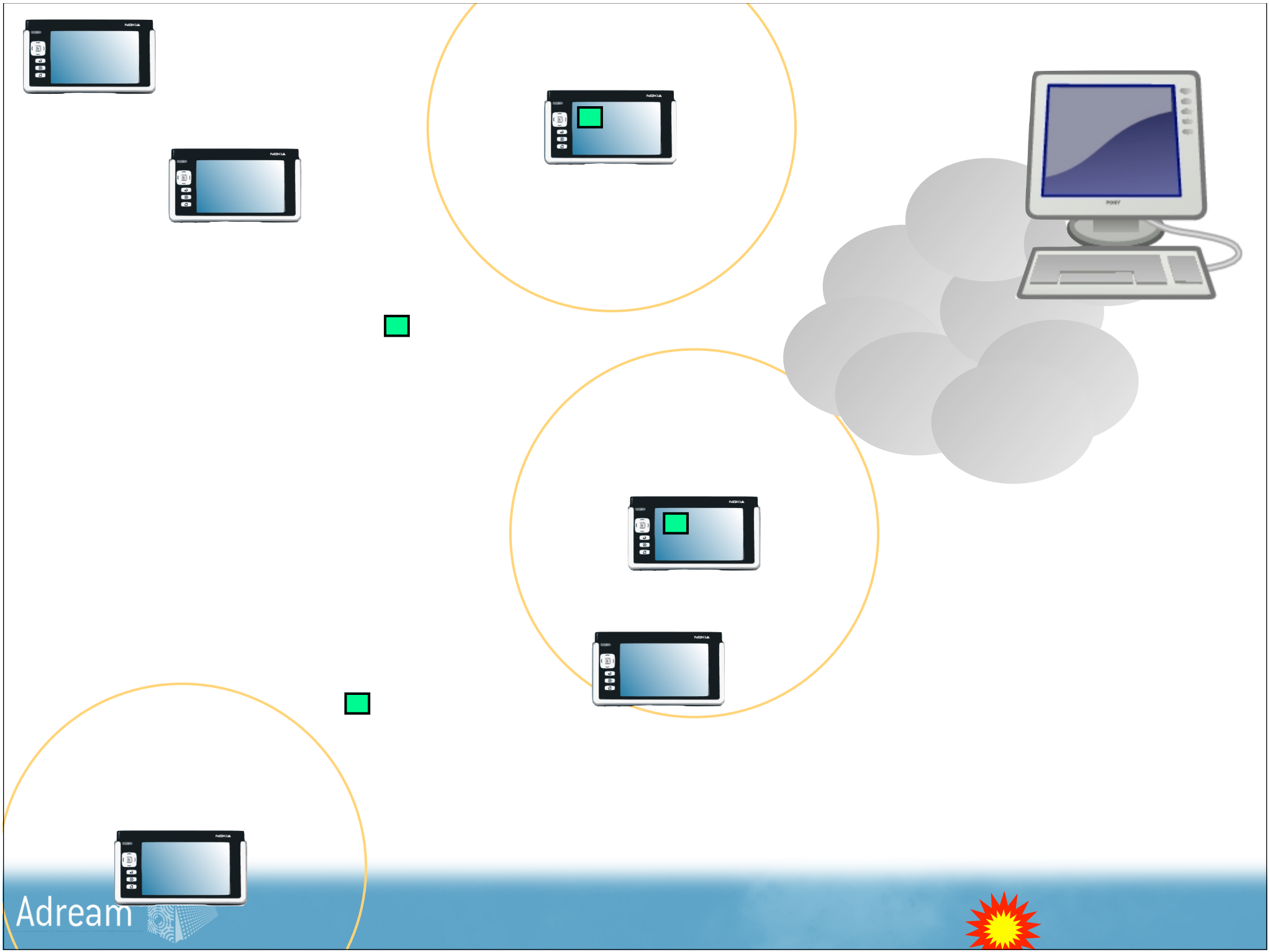


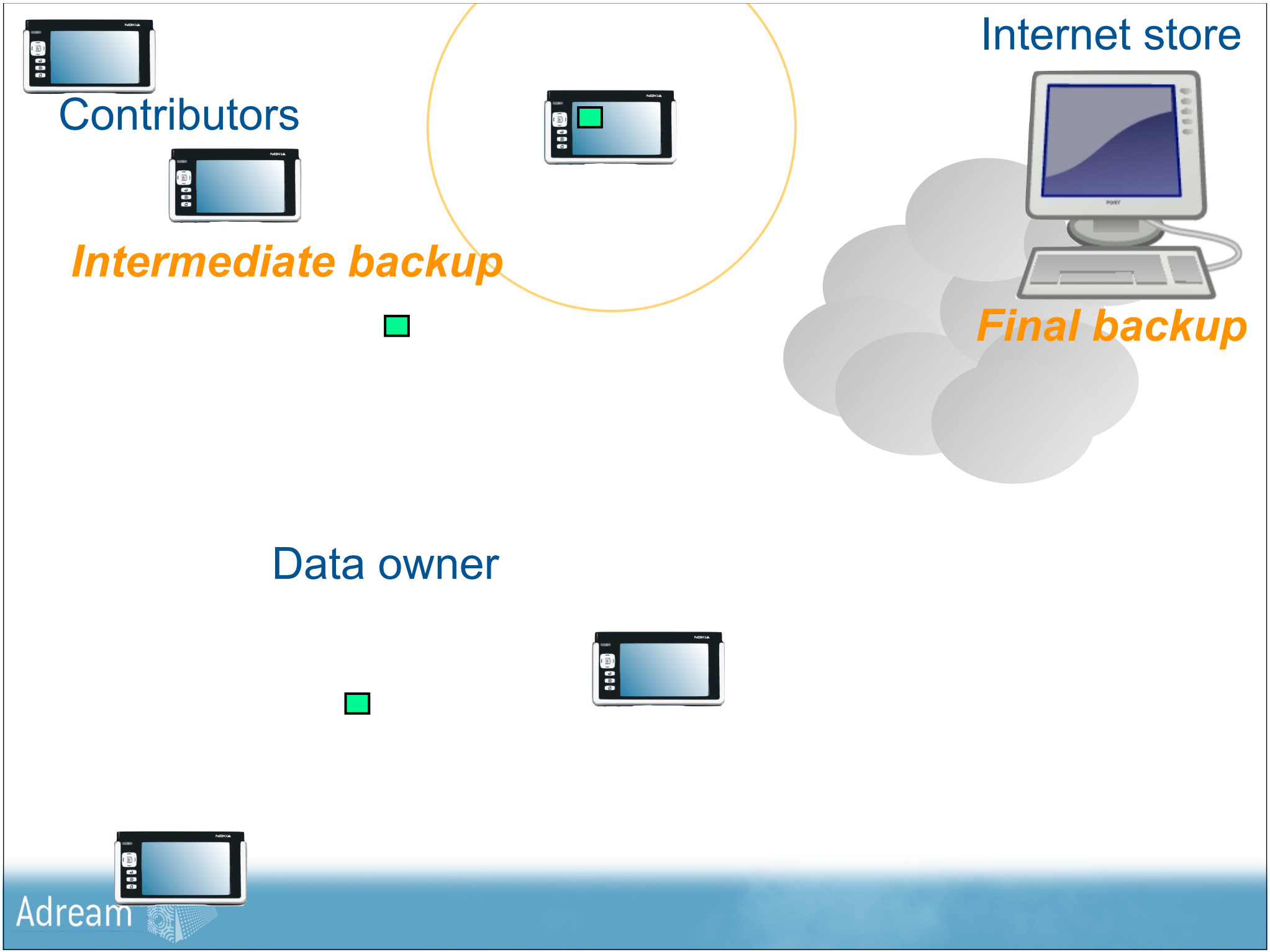
Sparse-connectivity model


Sparse-connectivity model
+ intermittent access to fixed infrastructure
Adream

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

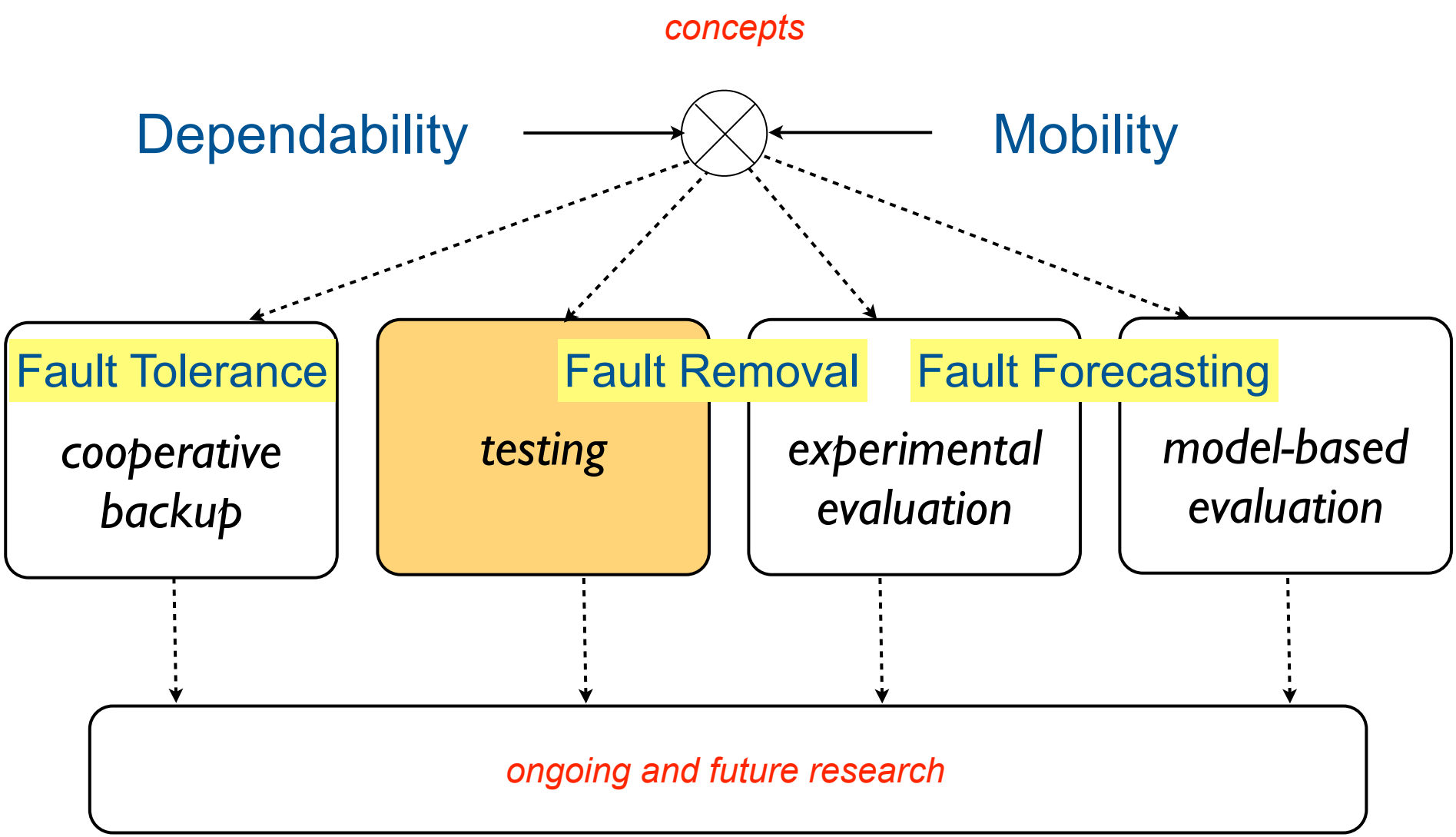

NOKIA
NOKIA
NOKIA
NOKIA
NOKIA
NOKIA
SONY
Adream


Contributors
Intermediate backup
Internet store
Final backup
Data owner
Adream

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

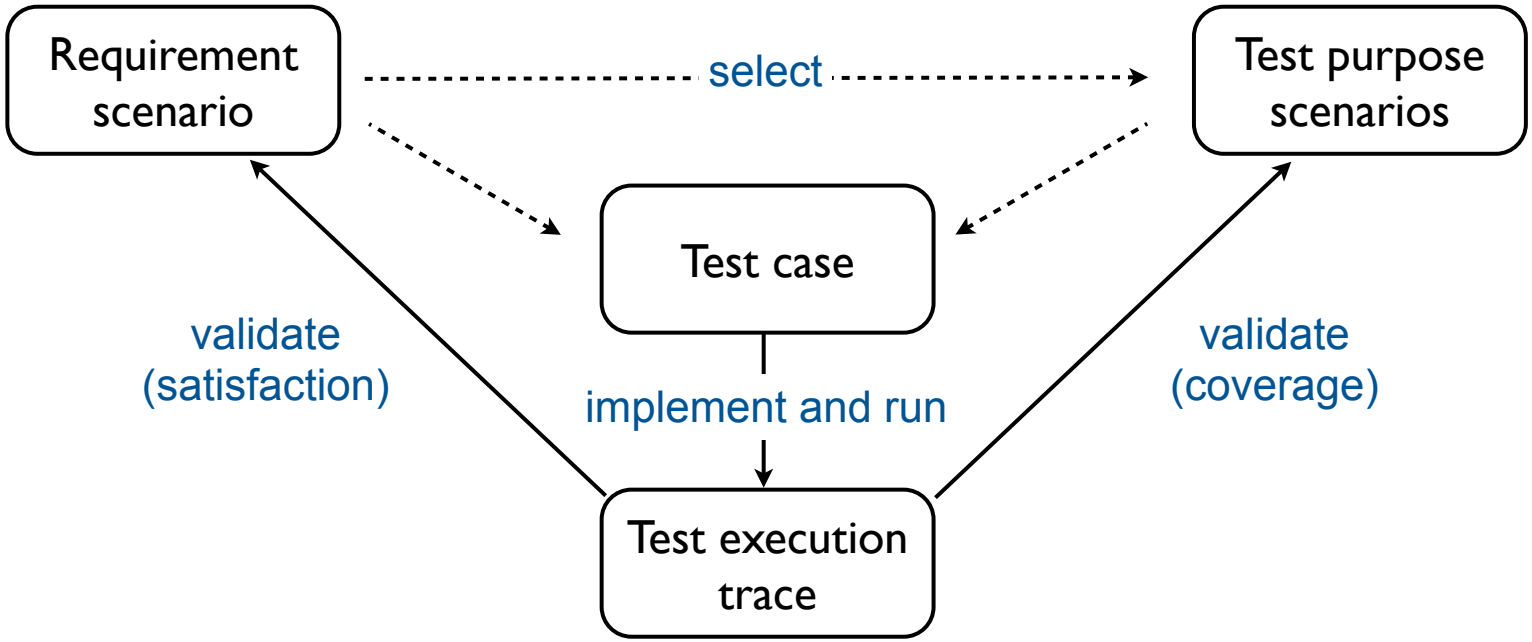
Roadmap


concepts
Dependability
Mobility
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

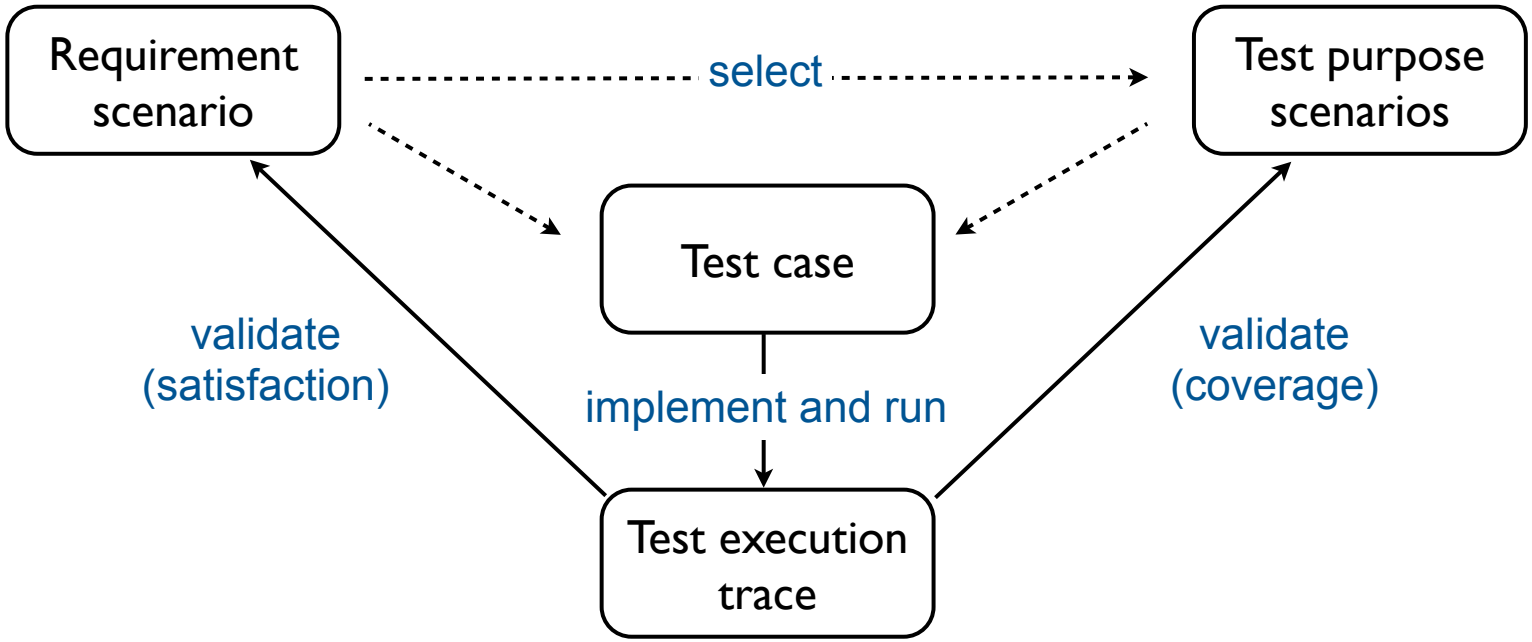
Test case: interaction of test components and SUT, verdict assignment

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

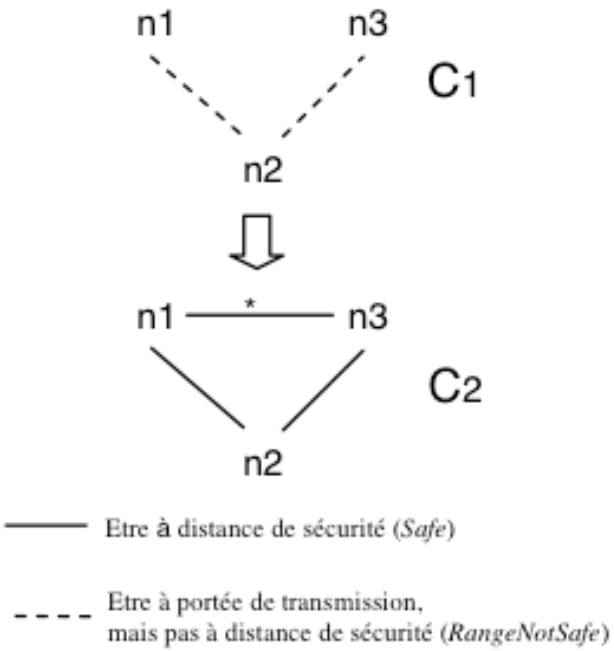
Scenario-Based Testing



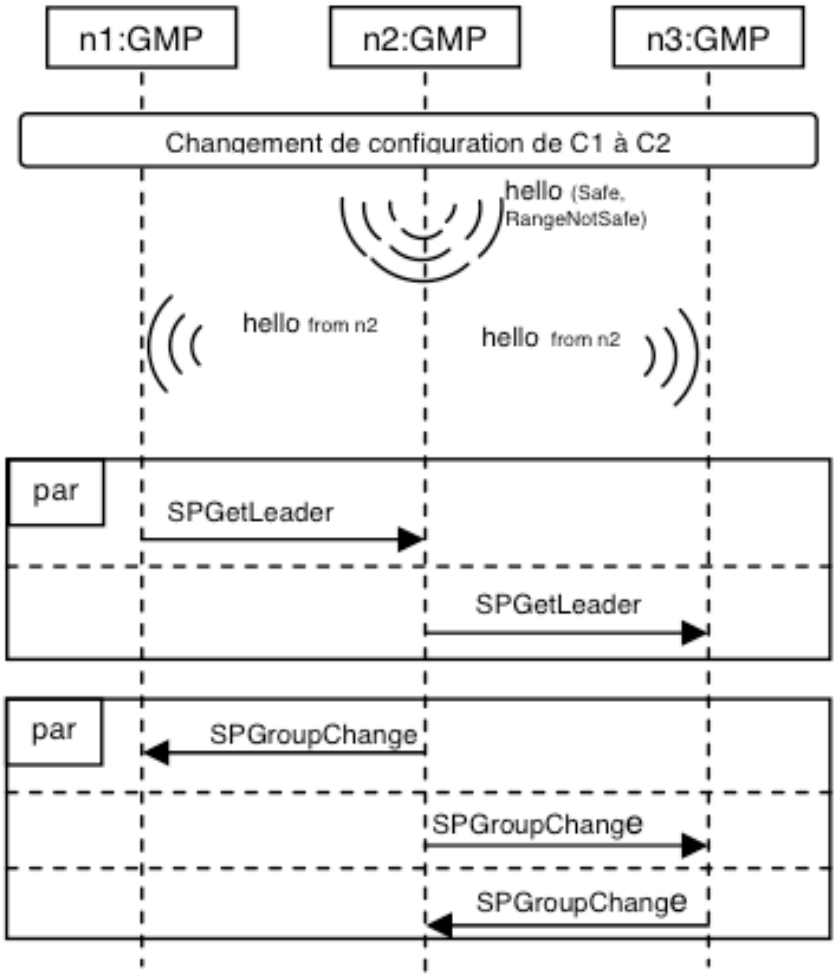
- **Graphical scenario language:**
  - UML sequence diagrams
  - plus mobility extensions:
    - neighborhood broadcast
    - system topology
    - topology changes

GMP Test Purpose Example

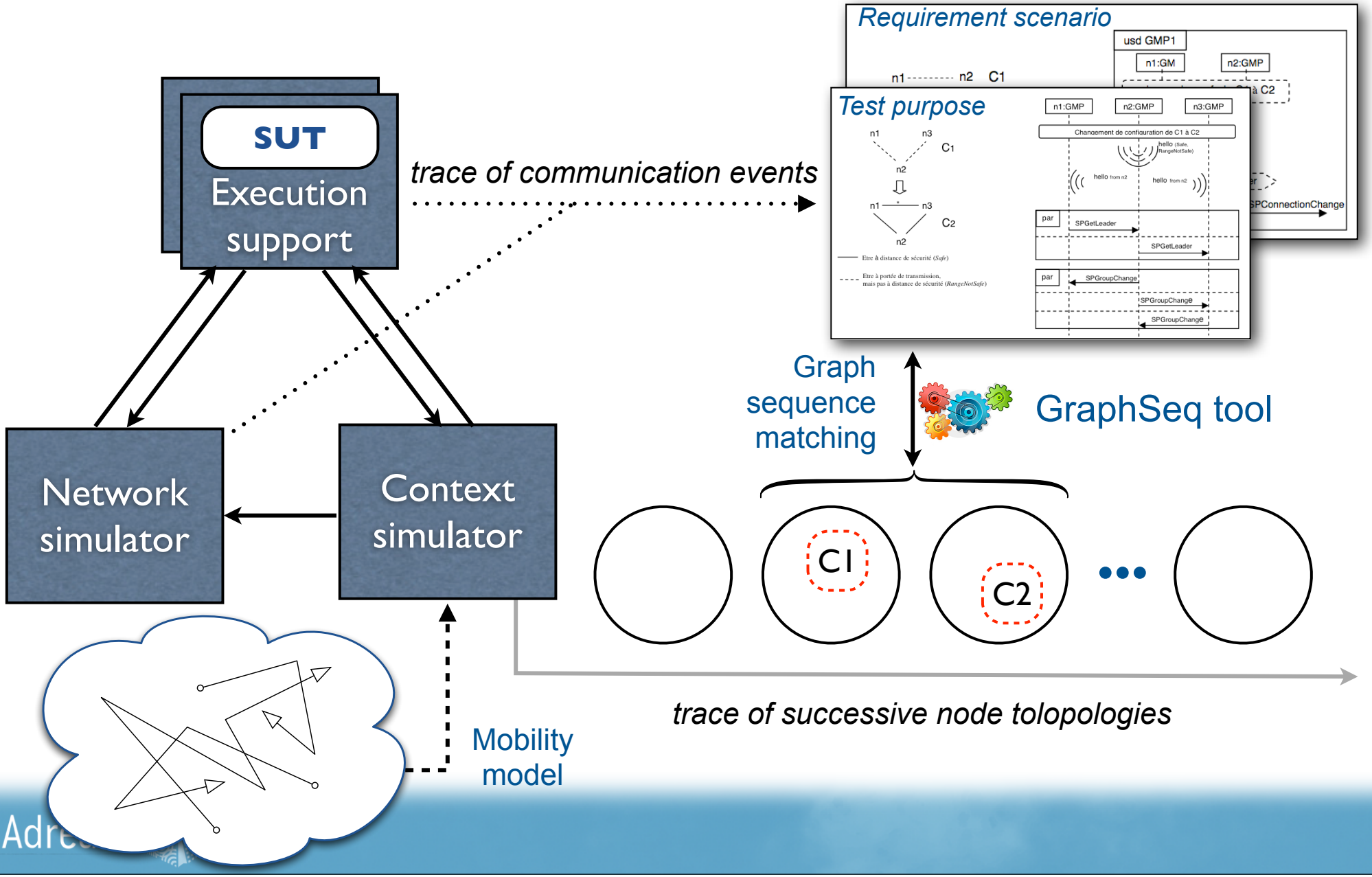
spatial view



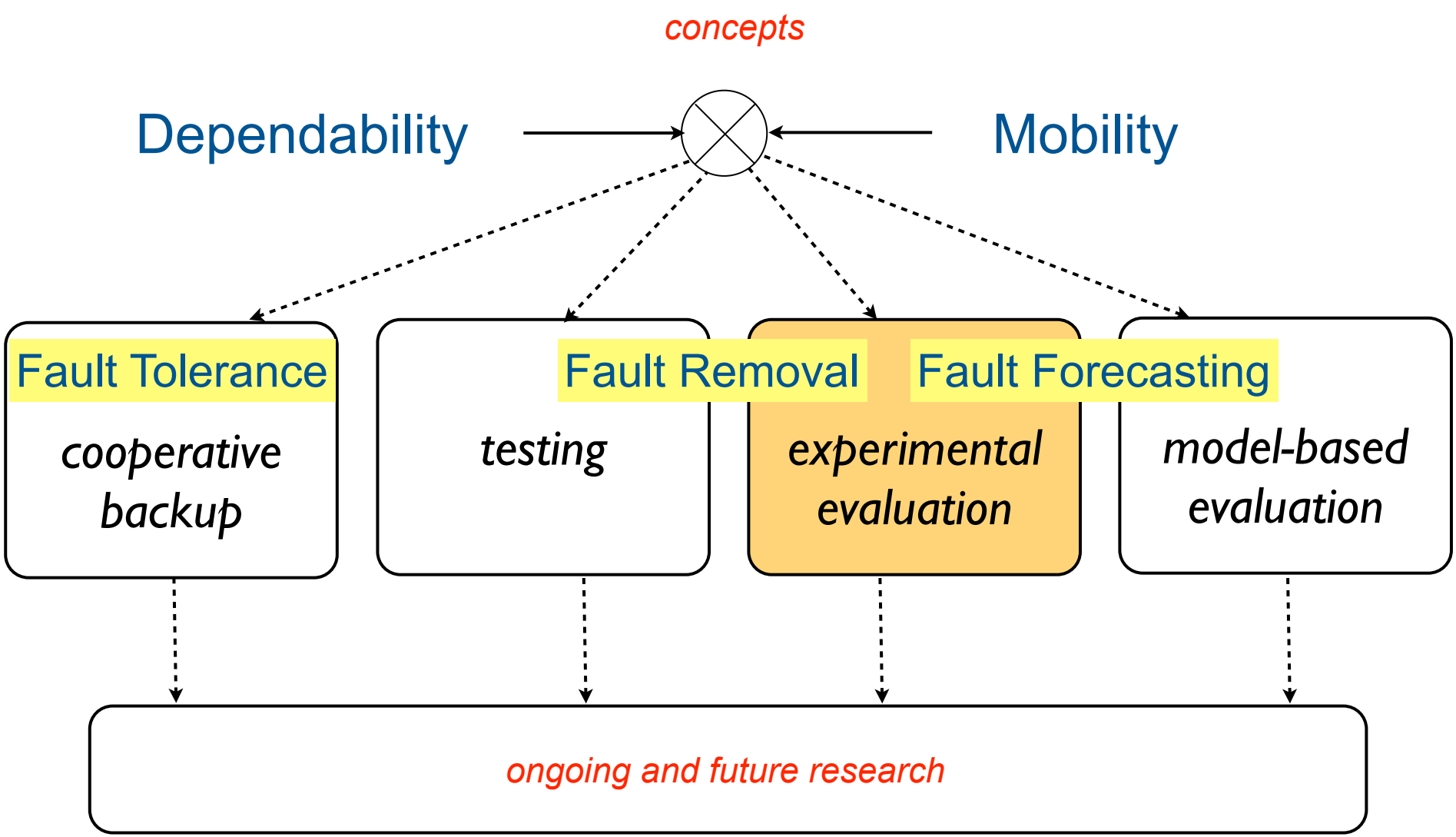
event view



Passive Testing Environment



Roadmap


concepts
Dependability
Mobility
Fault Tolerance
cooperative backup
Fault Removal
testing
Fault Forecasting
experimental evaluation
model-based evaluation
ongoing and future research

Experimental Evaluation in Mobile Setting

Simulated mobile system ⟷ **Real mobile system**

- ☺ cheap
- ☺ repeatable
- ☹ abstraction of reality
- ☹ boring

- ☹ 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

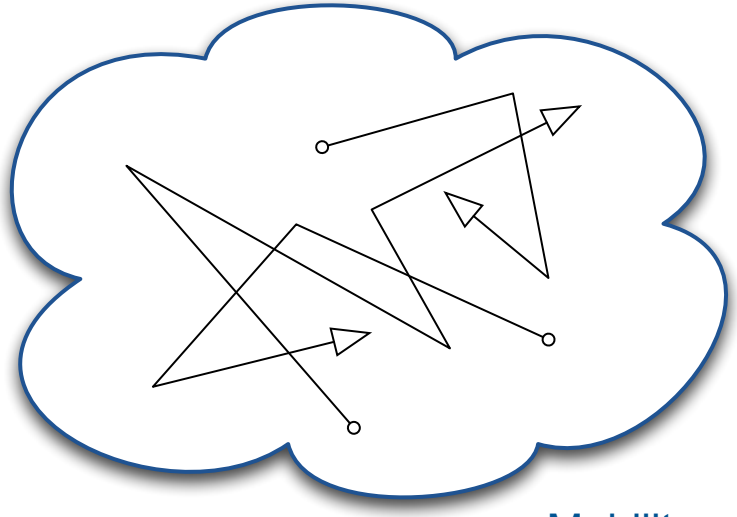
Scaled model of mobile system

- ☺ within reach of funding agencies
- ☺ quasi-repeatable
- ☺ real hardware/software environment
- ☹ scaling innaccuracies
- ☺ great fun!

Scaled Mobility Platform

Feature	Real system		Scaled model	
Wireless communication range	WiFi	100 m	2 m	WiFi + 26dB attenuators
Position-awareness accuracy	GPS	5 m	10 cm	Cortex motion capture system
Node size	Road vehicules	a few meters	a few decimeters	Lynxmotion 4WD rovers + laptops
Node speed		tens of km / hour	tens of dm / sec	

Mobility Representation



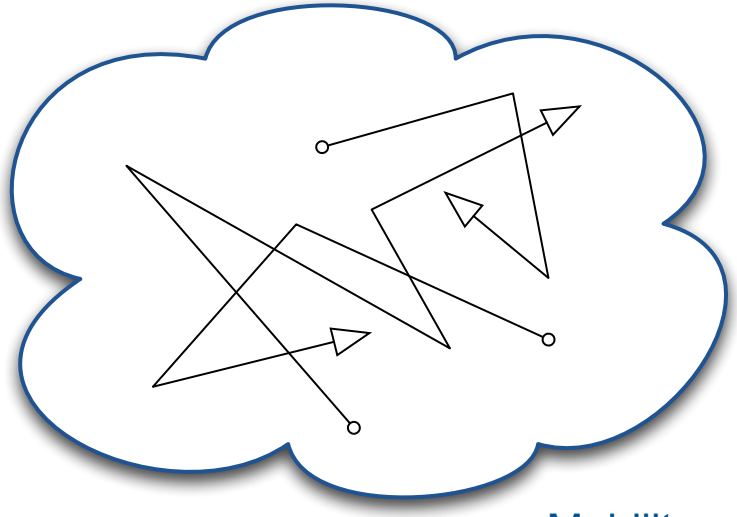
Mobility model

- **Physical tracks**
  - itinary + 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 beween vehicules
  - can be queried should accident occur

Mobility Representation



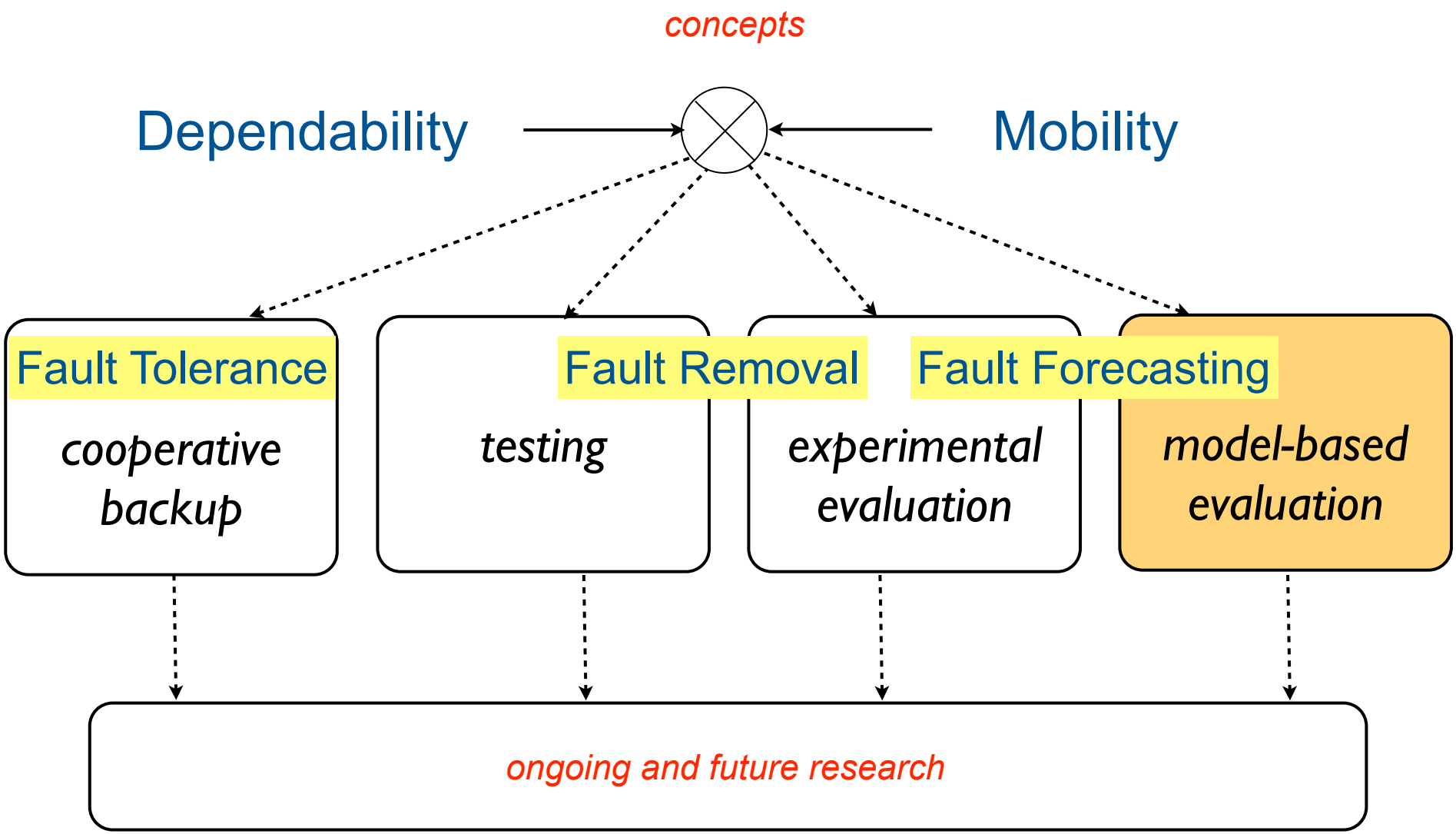
Mobility model

- **Physical tracks**
  - itinary + event-triggering waypoints drawn on floor using tape
- **Virtual tracks**
  - software-implemented itinary and velocity profiles using positioning service

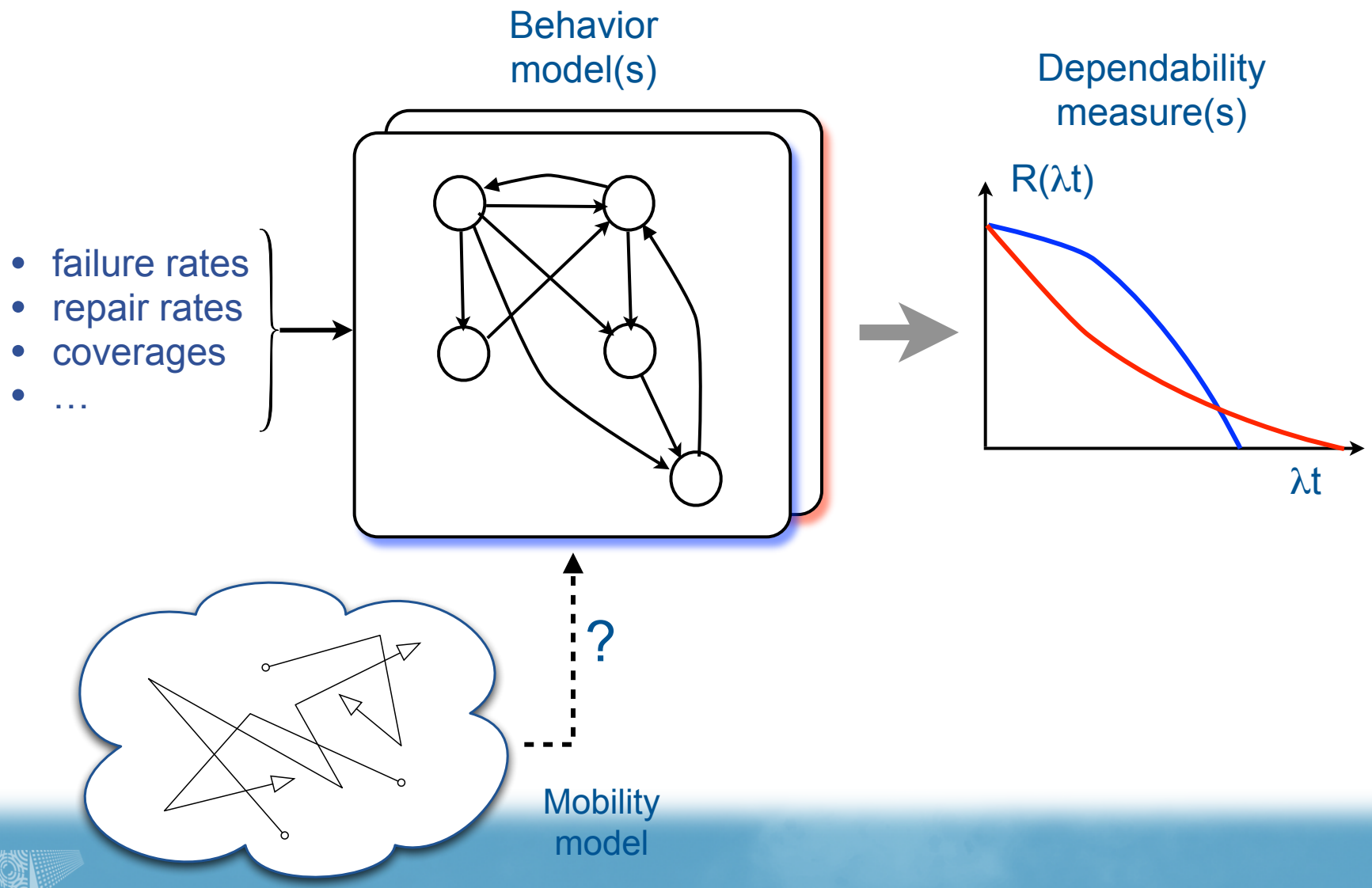
A Real Experiment

- **Scaled implementation of a distributed black-box application** (EU Hidenets project)
  - critical data backed-up cooperatively beween vehicules
  - 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

Roadmap


concepts
Dependability
Mobility
Fault Tolerance
cooperative backup
Fault Removal
testing
Fault Forecasting
experimental evaluation
model-based evaluation
ongoing and future research

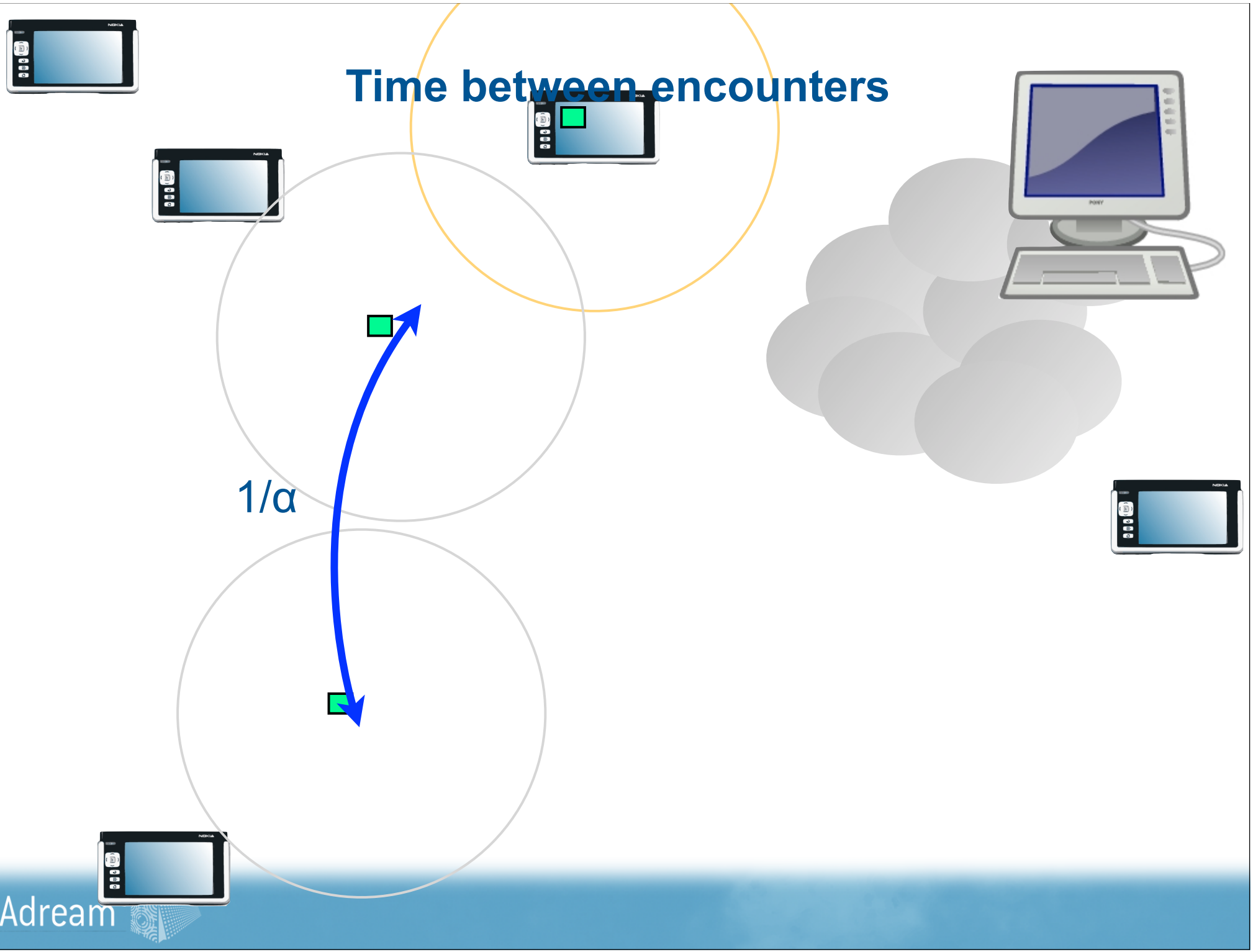
Model-based Evaluation in Mobile Setting



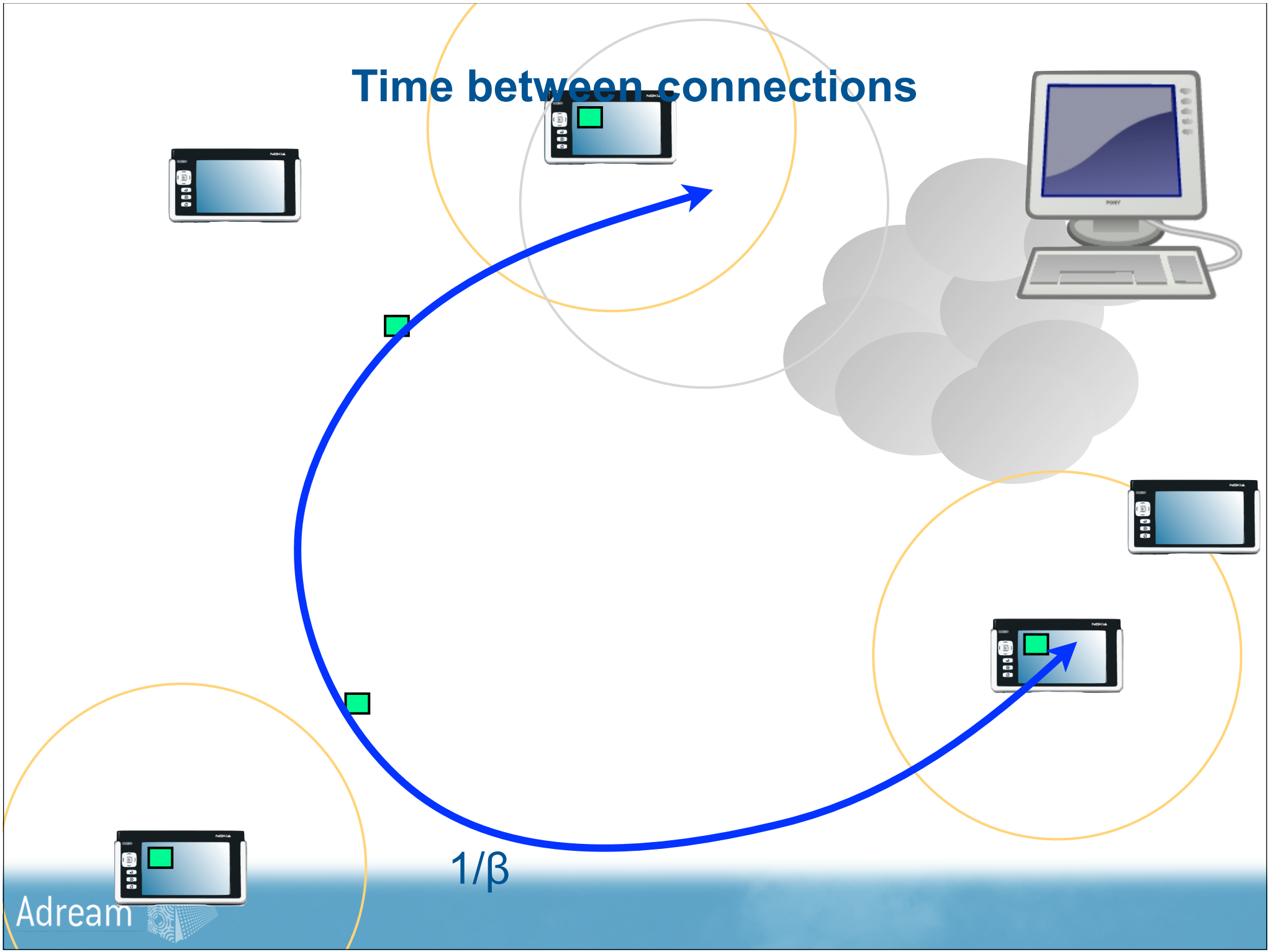
Dependability of Cooperative Backup

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

Time between encounters



Time between connections



Dependability of Cooperative Backup

Back-up process model

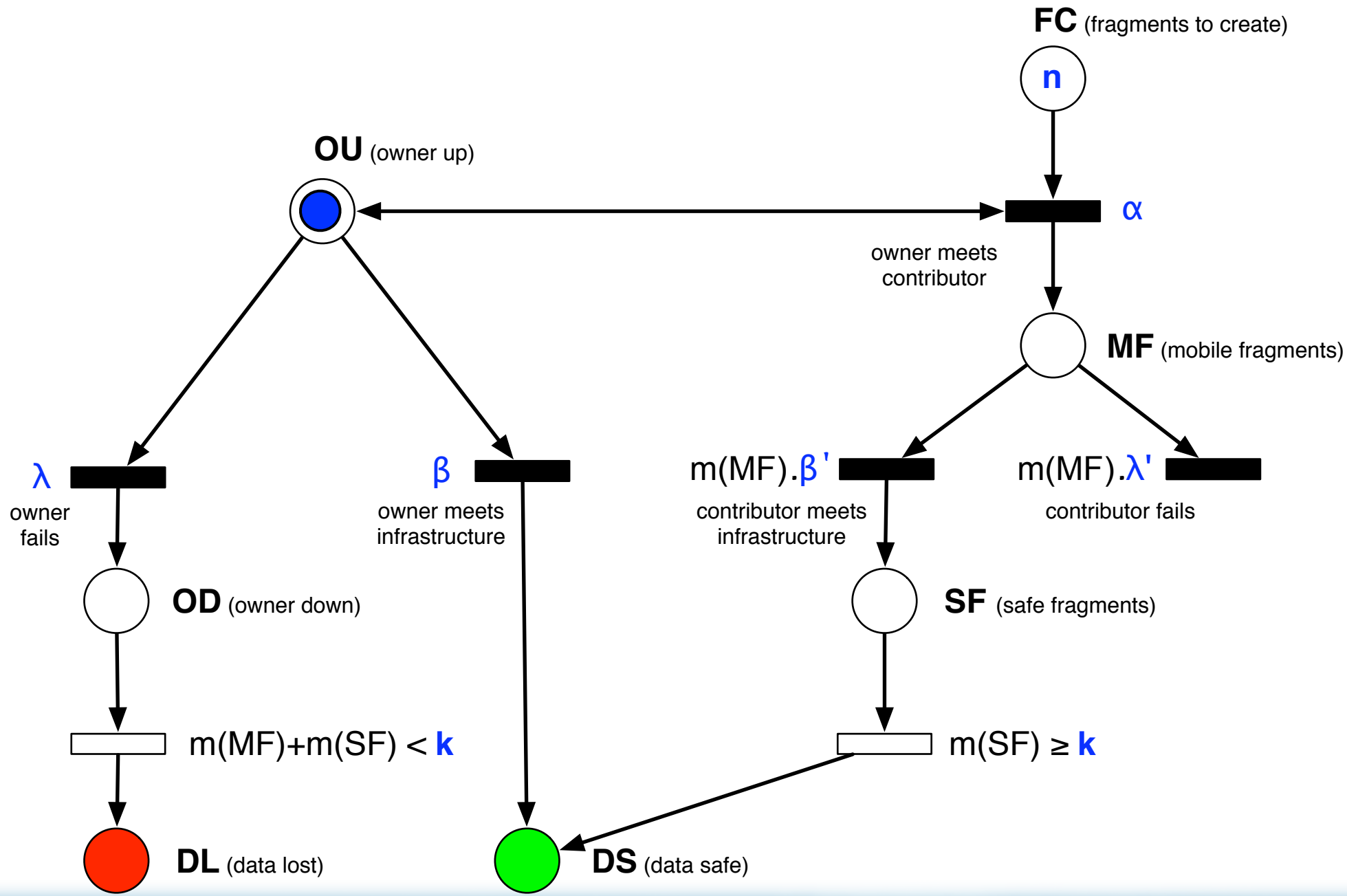
- (n,k) erasure code: up to n fragments sent to contributors
- data safe ⇨ original data or k fragments have reached Internet store
- data lost ⇨ data owner and contributors failed before k fragments reached Internet store

Device failure model

- crash failures
- stochastic process
- exponential distribution (rate λ)

Device mobility model

- stochastic processes
- exponential distributions
  - encounters with other devices (rate α)
  - connections to Internet (rate β)

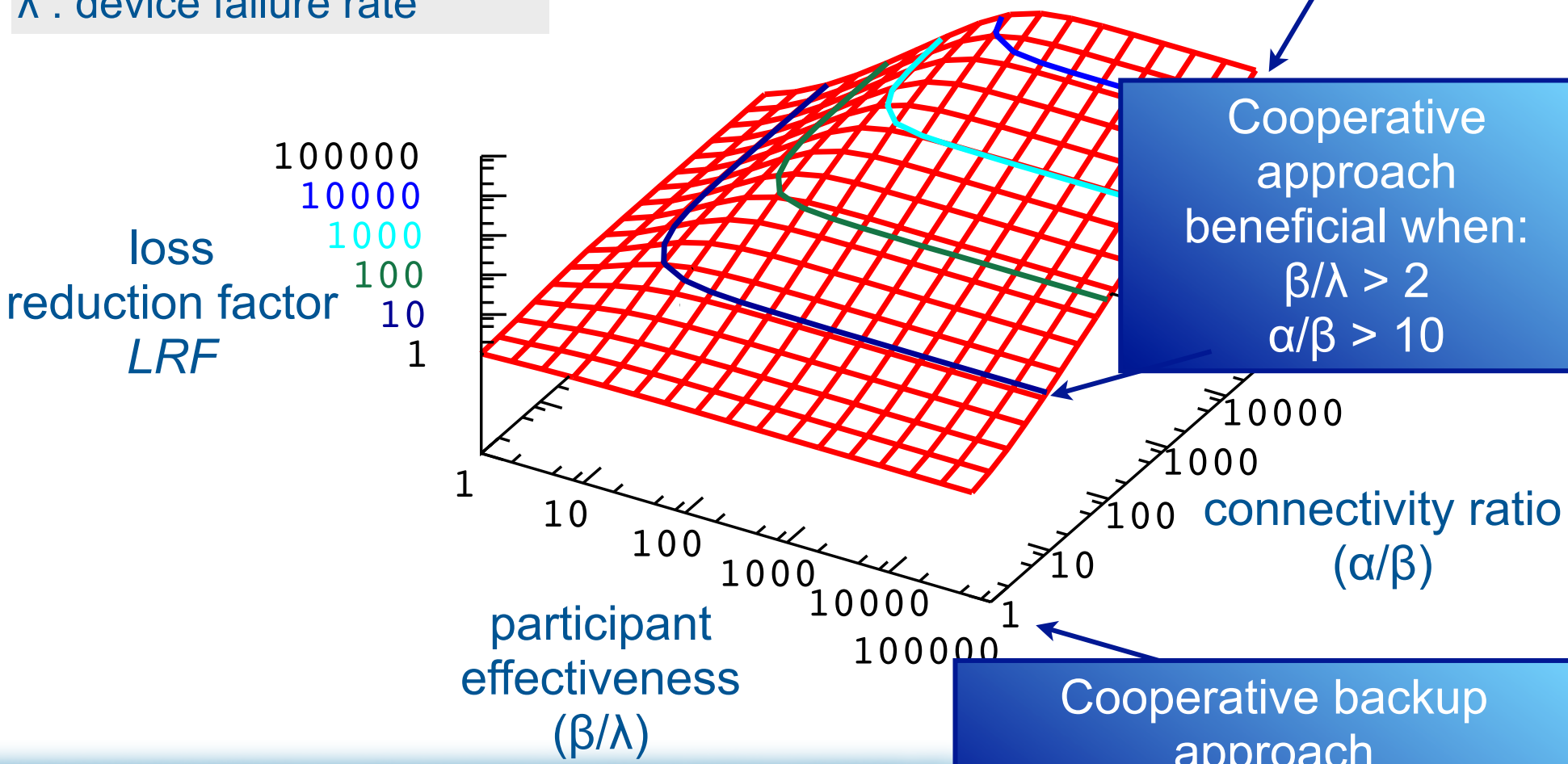

FC (fragments to create)
n
OU (owner up)
α
owner meets contributor
MF (mobile fragments)
λ
owner fails
β
owner meets infrastructure
m(MF).β'
contributor meets infrastructure
m(MF).λ'
contributor fails
OD (owner down)
SF (safe fragments)
m(MF)+m(SF) < k
m(SF) ≥ k
DL (data lost)
DS (data safe)

LRF vs. basic parameters

$(n,k) = (3,2)$

α : device encounter rate
β : internet connection rate
λ : device failure rate

Data loss probability decreased by up to α/β



Cooperative approach beneficial when:
β/λ > 2
α/β > 10

Cooperative backup approach useless when α/β < 1

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