Availability Modelling of a Virtual Black-Box for Automotive Systems

Ossama Hamouda, Mohamed Kaâniche, Karama Kanoun

LAAS-CNRS

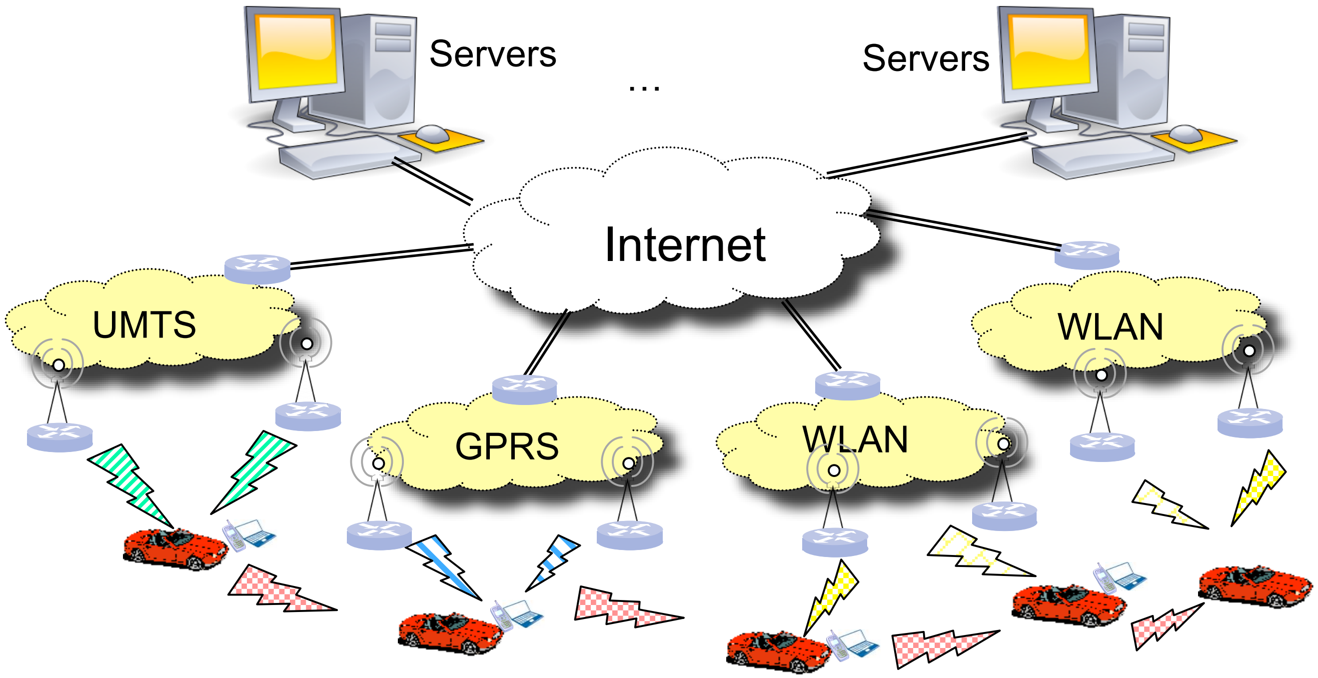
HIDENETS
HIghly DEpendable IP-based NETworks and Services

Information Society Technologies

SIXTH FRAMEWORK PROGRAMME

SERENE-2010
2nd International Workshop on Software Engineering for Resilient Systems
15-16 April 2010, Birkbeck College, London, UK

Context



- Wireless and mobile technologies for automotive applications
  - Car-to-car communication with server-based infrastructure
- Increase traffic capacity and safety
- Dependability challenges: design and assessment

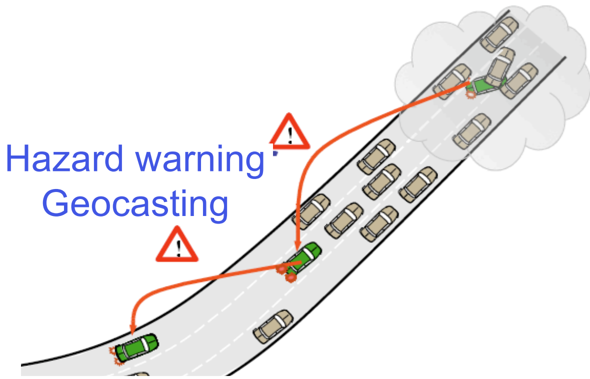
Challenges

- Dynamicity/mobility
  - changing topologies and communication characteristics
- Heterogeneity
  - different technologies and QoS characteristics
- Complexity
  - large number of components and interactions
  - multiple failure modes and fault classes
- Performance/dependability/security tradeoffs

☞ Holistic dependability evaluation approach integrating analytic, simulation and measurement based techniques

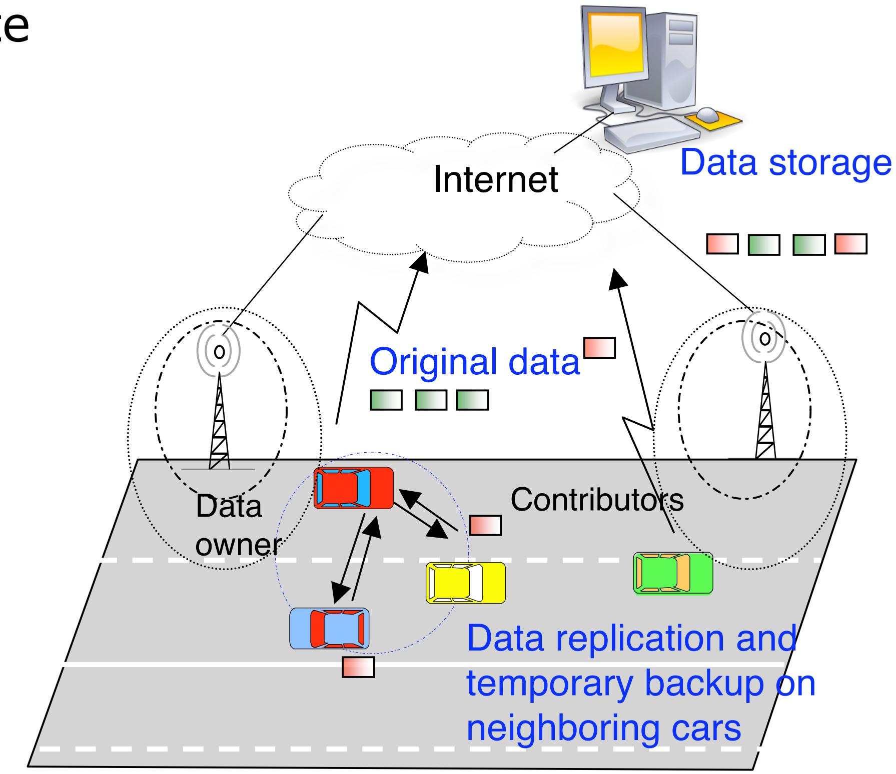
Applications

- Local hazard warning
  - Information gathering and dissemination (congestion, state of the road, accident, etc.)



- Platooning
  - Automated highway system

- Virtual black box



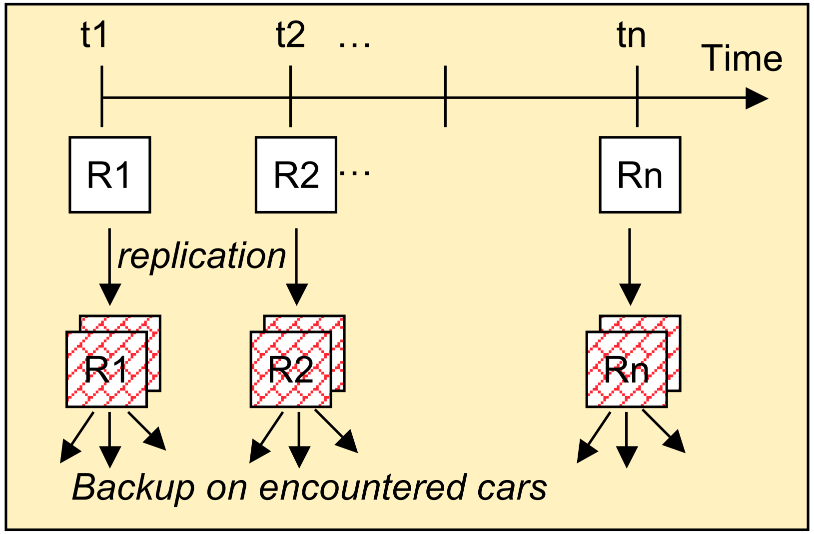
Virtual Black Box Application (VBB)

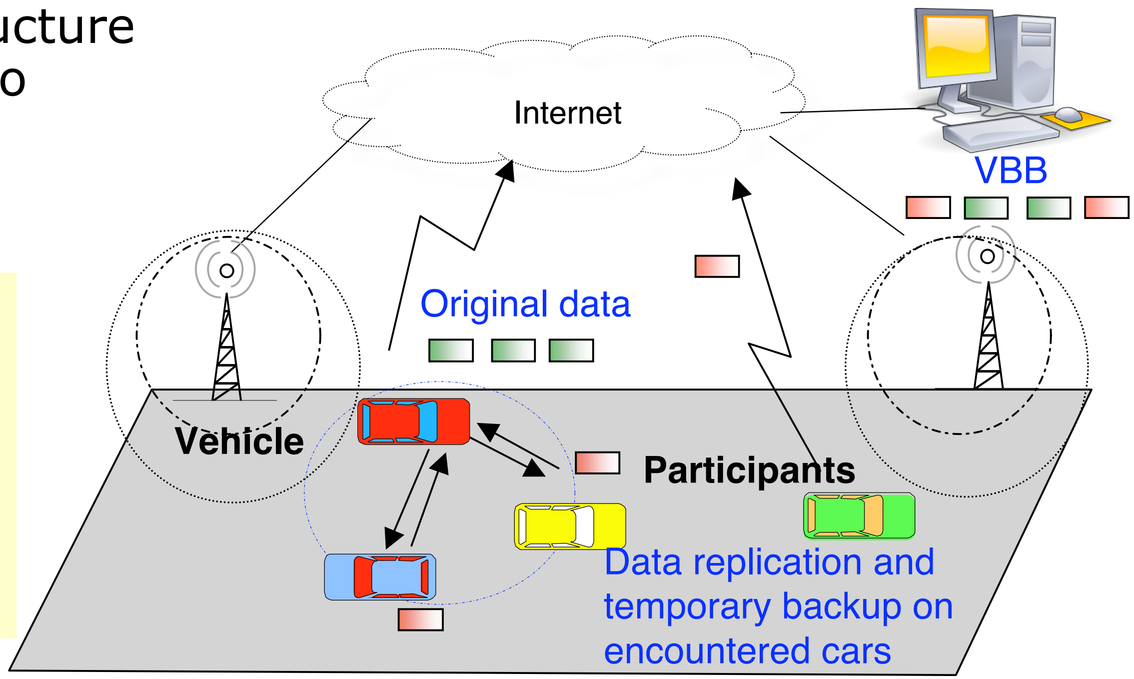
- Objective
  - Collect relevant information related to a vehicle and its environment, in a manner similar to the black box of an aircraft
    - Replay historical data in the event of an accident
  - Software-based data storage on the fixed infrastructure
  - Need to protect data against accidental and malicious threats ➠ use data replication

- Dependability attributes
  - Data availability
  - Data integrity
  - Data confidentiality

Scenario

- Data *Records* continuously collected and temporary stored on the vehicle
- VBB resident on the infrastructure
- To prevent data loss:
  - Data records are replicated and backed up on encountered cars (Participants)
  - Data stored on infrustructure when access available to Vehicle/Participants





When an accident occurs, the last z records gathered are sufficient to analyze the accident (or at least r among these z)

Data Records Replication

- Replication strategies
  - Replication by duplication
    - Create full copies of the data record
  - Replication by fragmentation: Erasure codes
    - Suitable to ensure data availability and confidentiality

- Erasure code (n, k)
  - Generates n fragments of the data record that are disseminated to encountered cars.
  - k fragments are sufficient to restore the original record
  - (n-k) fragments loss can be tolerated (besides original record)
  - n = k =1: replication by duplication
  - k ↗↗ ➠ confidentiality ↗↗

Dependability Modeling

- VBB unavailability assessment
- Sensitivity analyses
  - Replication strategy: n, k
  - Number of records to analyze an accident: z, r
  - Other parameters
    - Rate of data loss (Vehicle /Participants): failure rate λ
    - Car-to-Car encounter rate : α
    - Car-to-Infrastructure connection rate: β
- Two step approach
  - Connectivity dynamics analysis
    - C2C and C2I encounter distributions and connection rates
  - Availability modeling based on stochastic models using the results of the connectivity analyses as an input

Analysis of connectivity dynamics

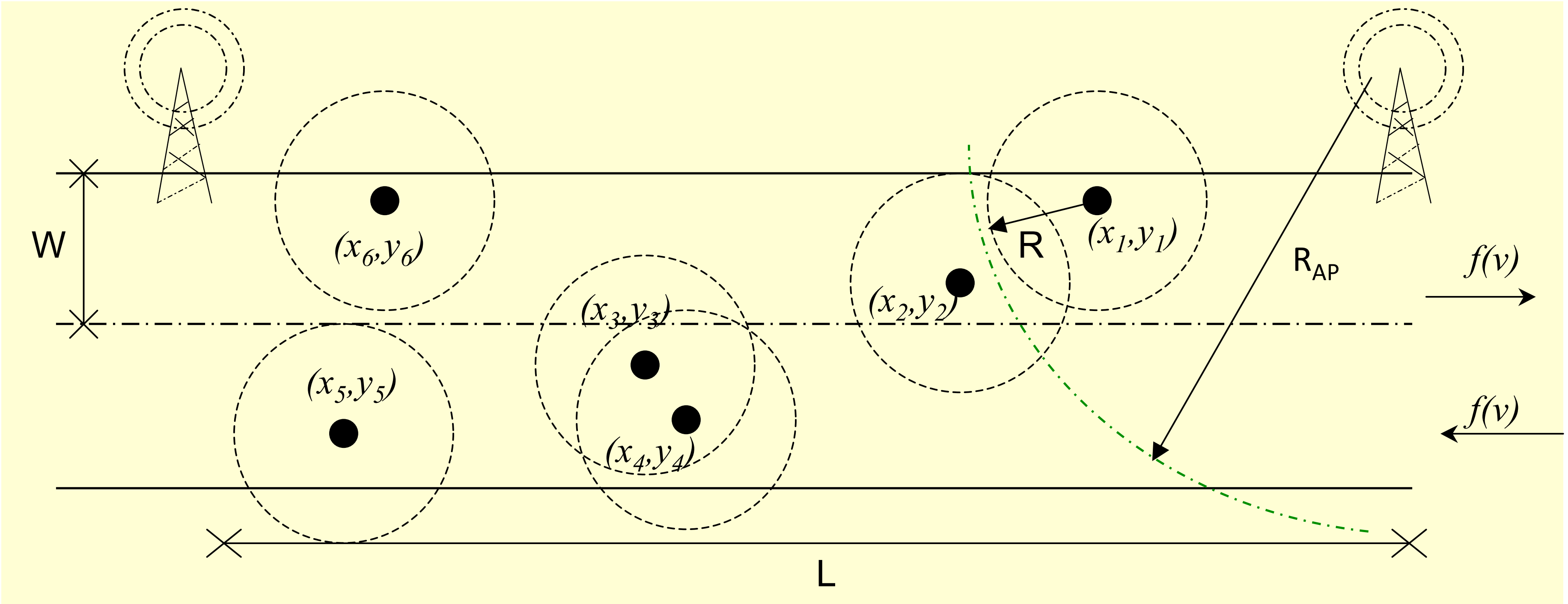
Techniques

- Analytical proofs
- Simulation
- Processing of publicly available mobility traces
  - CRAWDAD: http://crawdad.cs.dartmouth.edu
  - Multi-agent Traffic simulator developed by ETH Zürich
    http://www.lst.inf.ethz.ch/research/ad-hoc/car-traces

Conclusions

- C2C encounter times Distribution
  - Freeways: Exponential
  - Urban traffic: Pareto
- C2I encounter times Distribution
  - Exponential

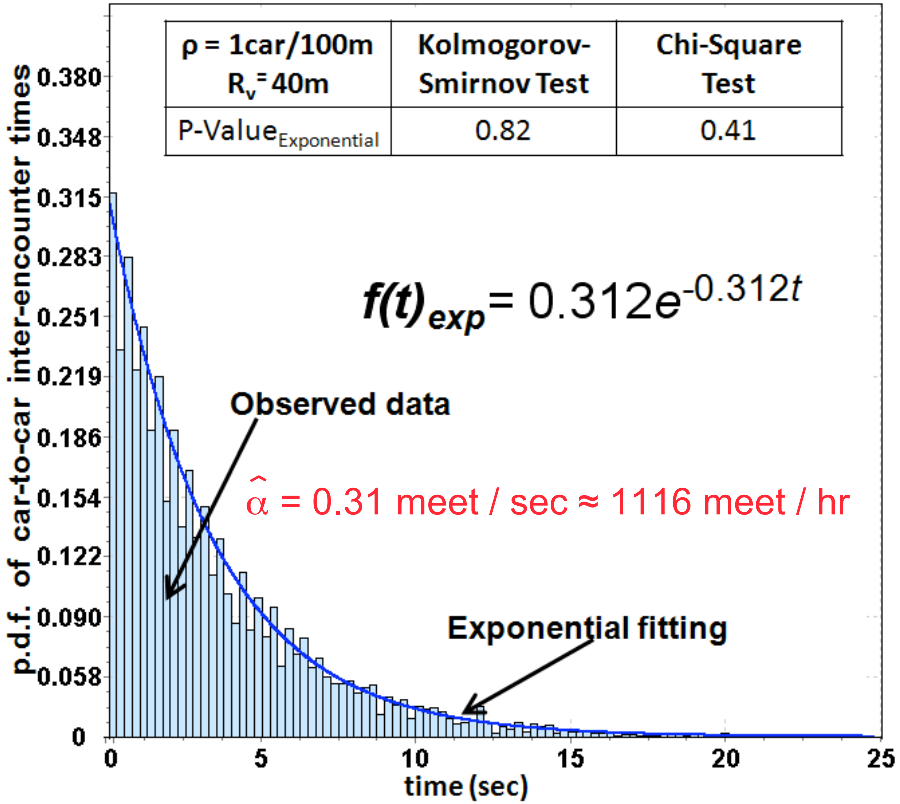
Simulation of a freeway scenario



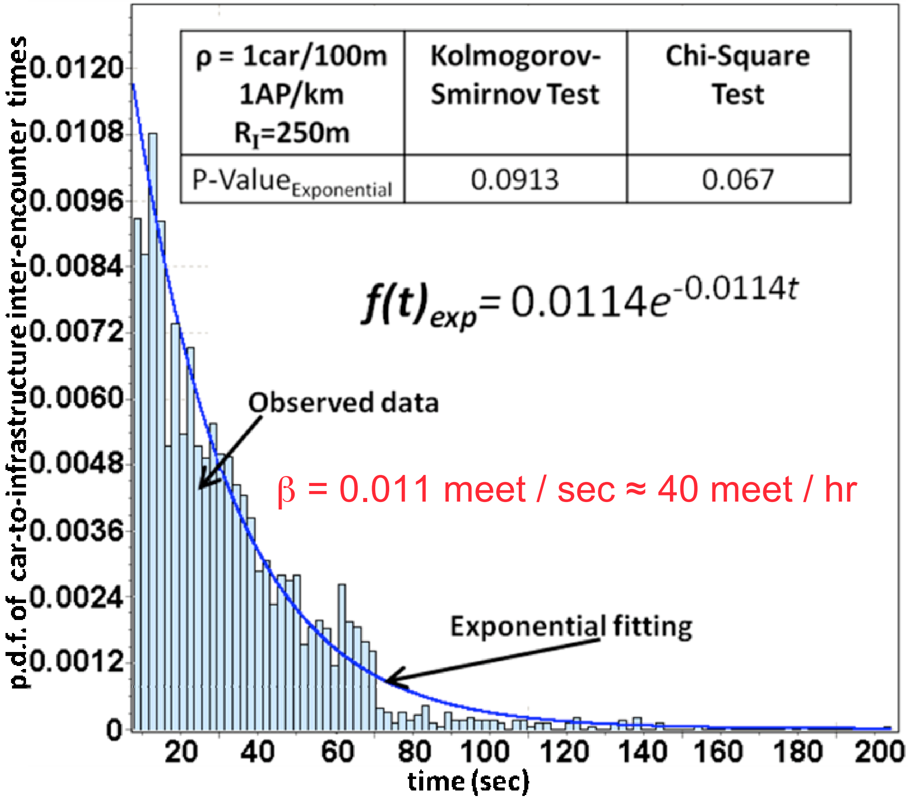
- Cars move independently according to speed distribution *f(v)*
  - opposite directions on upper and lower half
- Uniform Initial placement of cars (ρ: car density)
- Fixed communication radius for the cars: *R*

Example of results: freeway mobility scenarios

C2C encounter times



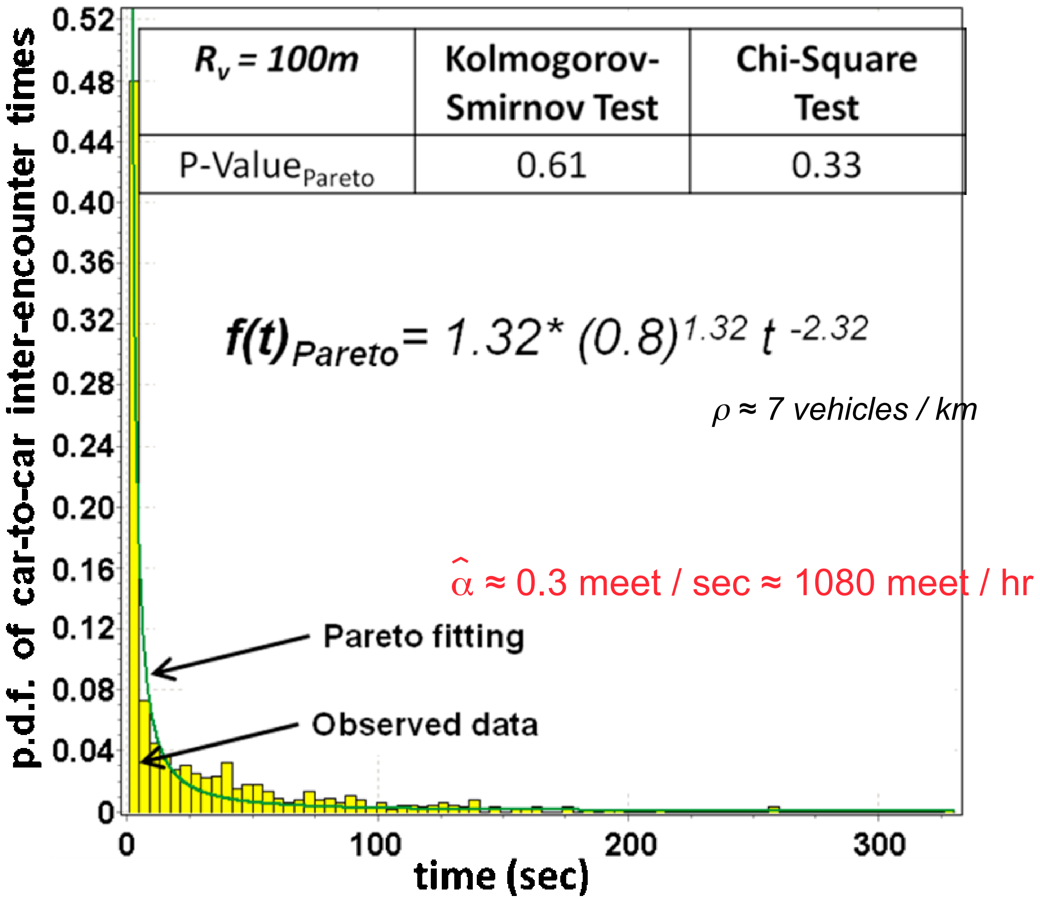
C2I encounter times



- Exponential distribution well suited to describe C2C and C2I encounter times

Urban mobility scenarios

CRAWDAD
mobility trace

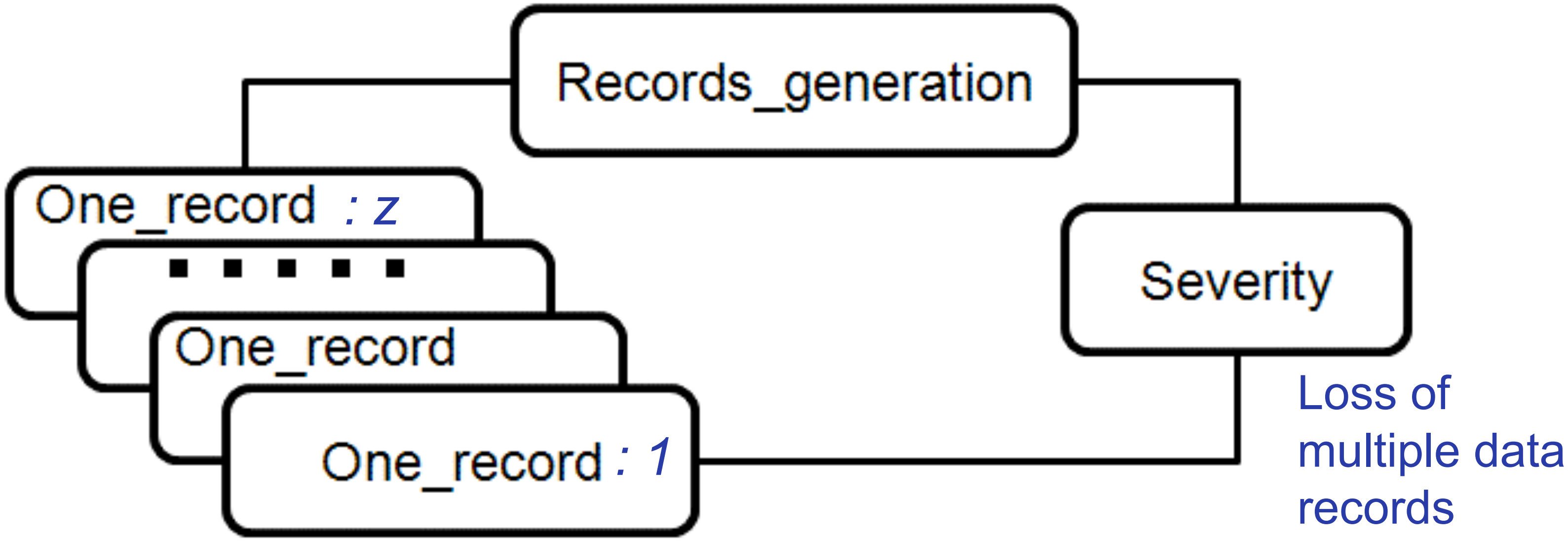


Pareto provides a better fit than the exponential distribution

Virtual Black Box availability modeling

- Unavailability measure: UA
  - Probability of data loss:
    - more than *r* data records among last generated *z* records lost
- Modeling assumptions
  - Failures: Data records loss times (Vehicle/Participants)
    - Exponentially distributed with rate λ
  - Mobility scenarios:
    - C2C encounter times:
      - Exponentially distributed with rate α (Freeways)
      - Pareto distributed (Urban traffic)
    - C2I encounter times: exponentially distributed with rate β
- Modelling formalism
  - Stochastic Activity Networks (SANs)
  - Möbius tool

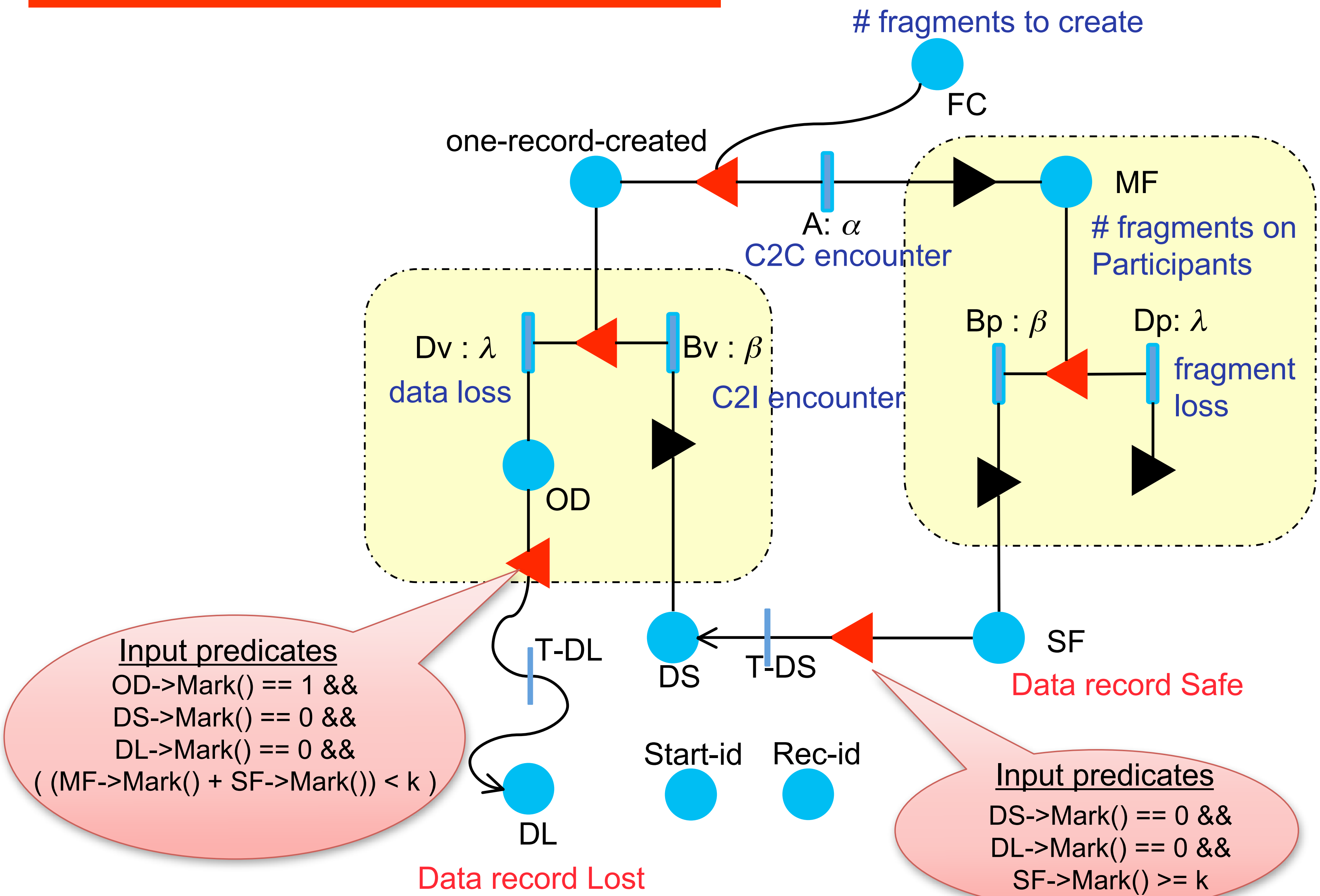
System Model



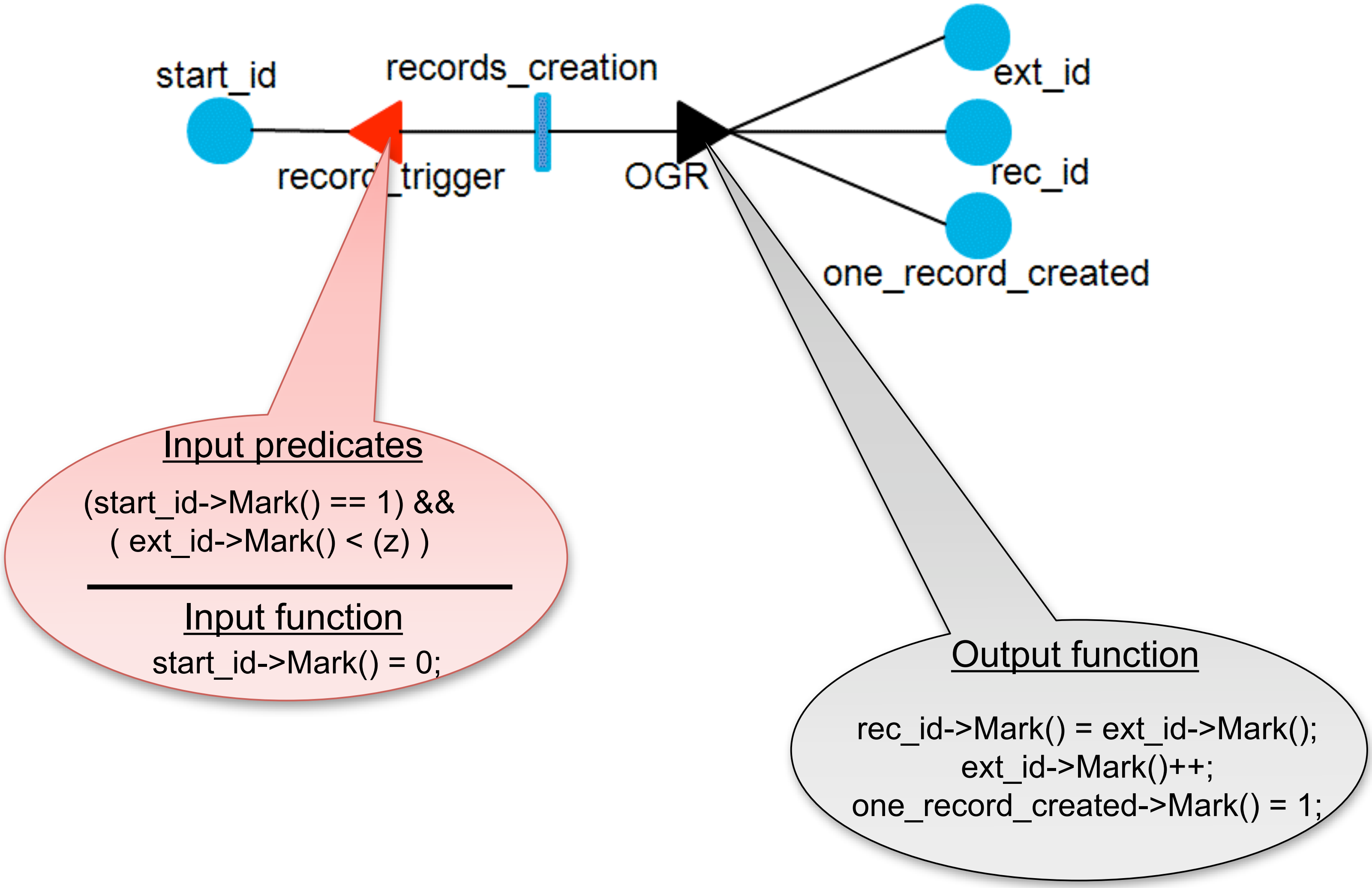
Single data record behavior:

- data loss
- Replication and storage at infrastructure

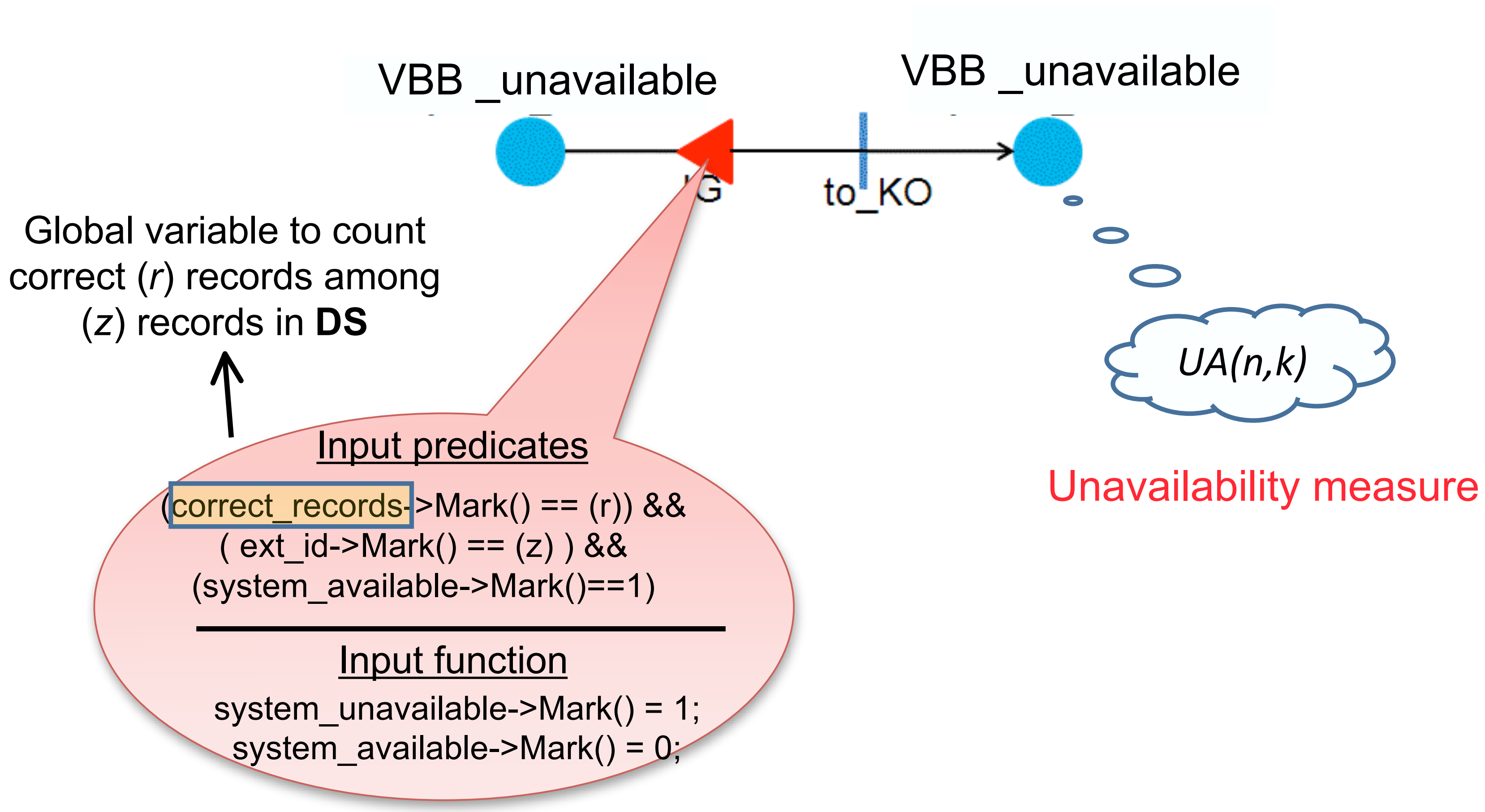
One_record submodel



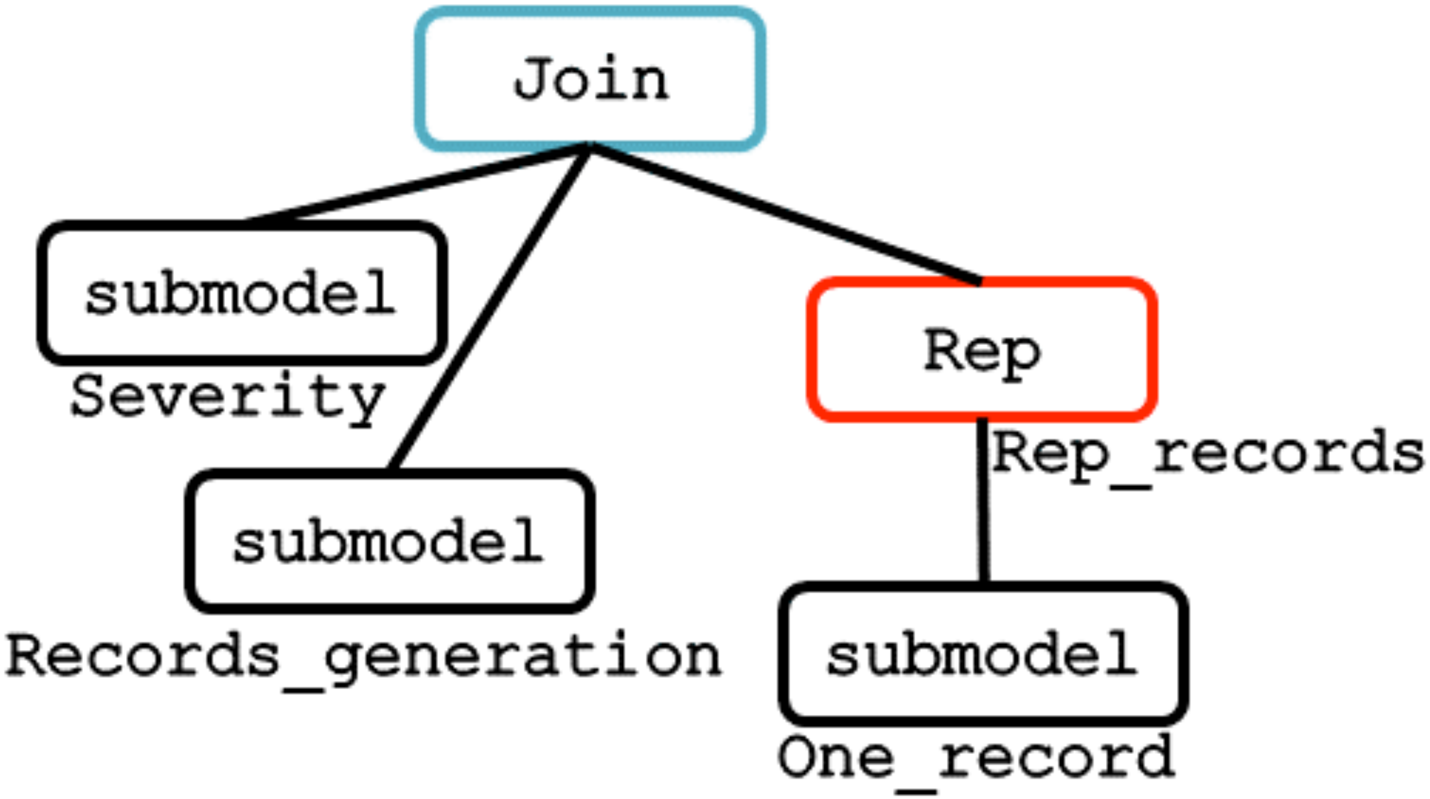
Record generation submodel



Severity submodel



SAN composed model

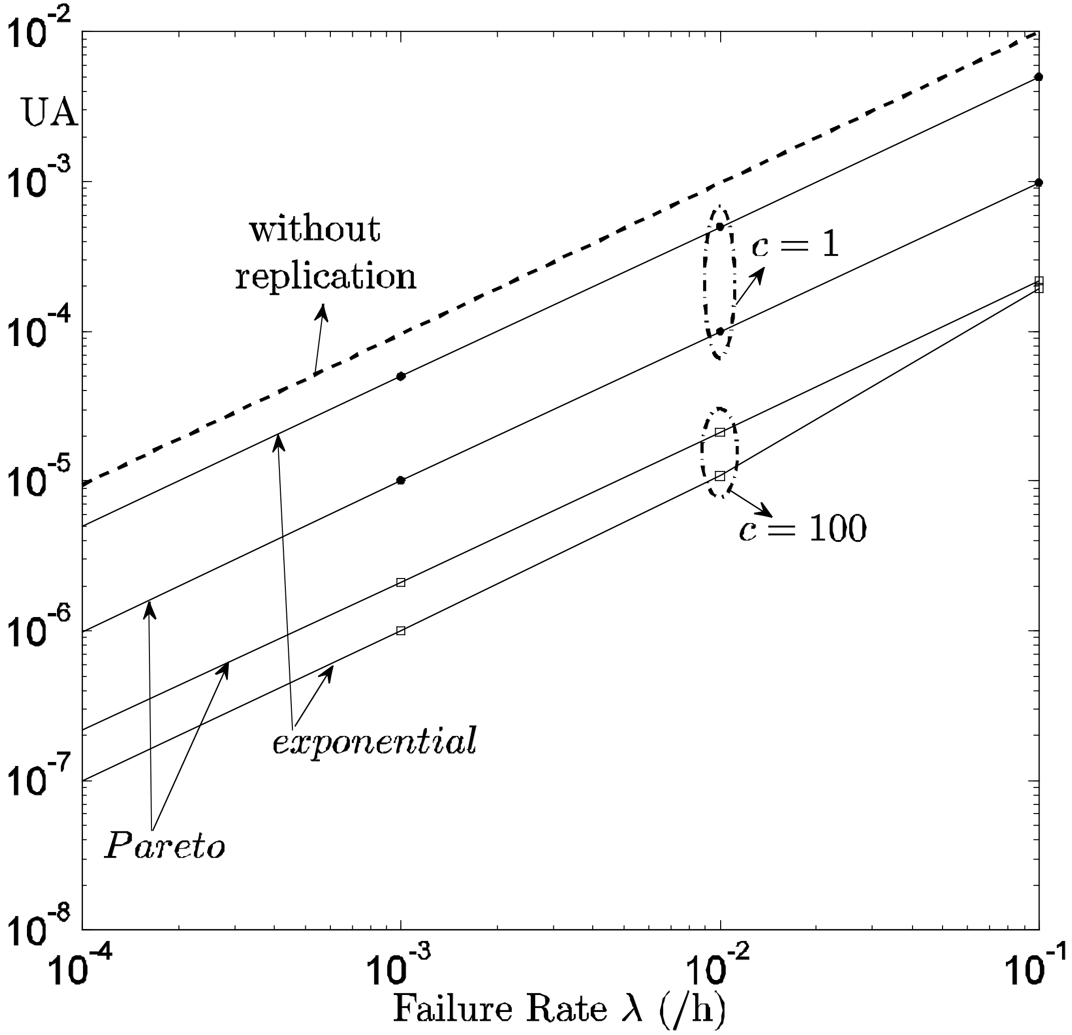


Results and sensitivity analysis

- Parameters

α	The vehicle-to-vehicle encounter rate
β	The connection rate to the fixed-infrastructure
c	The connectivity ratio = α/β (the rates at which vehicles meet relative to the rate at which connection to the fixed-infrastructure is possible)
λ	The rate at which data losses occur, on the Vehicle and the participants side (failure rate)
n , k	Parameters of the erasure code
r , z	Define the accuracy required of the historical information to analyse what happened when an accident occurs

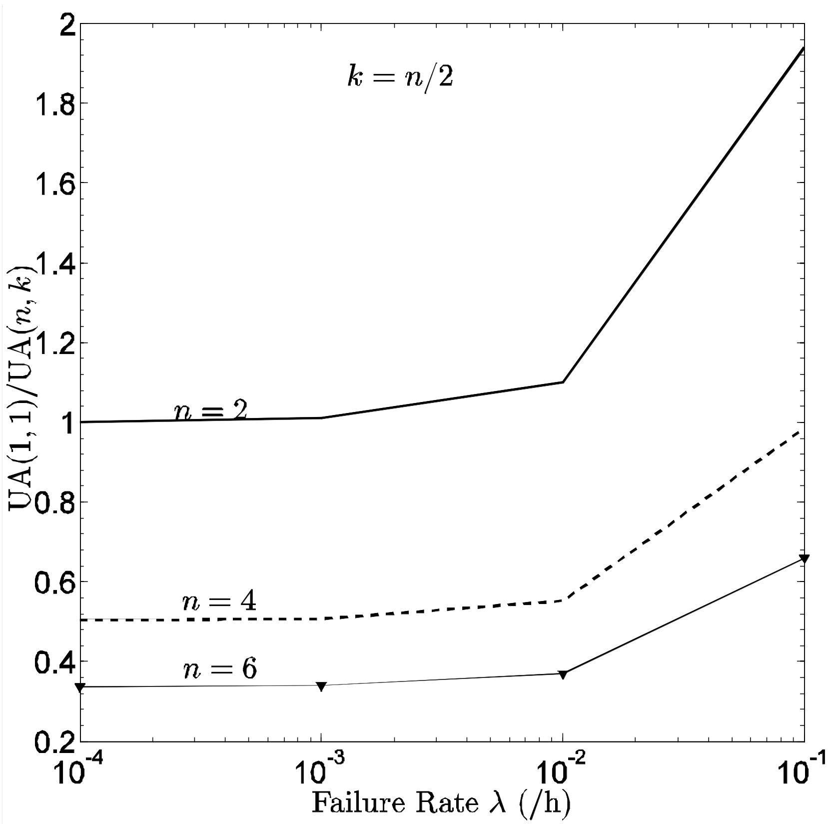
Unavailability of one data record



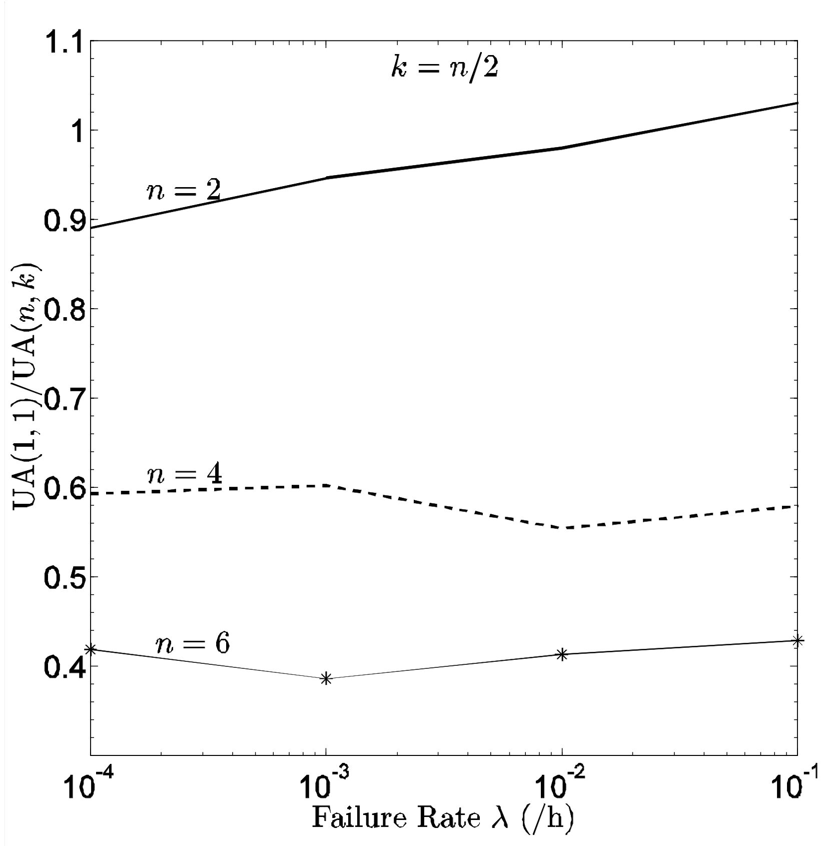
Exponential vs Pareto

Unavailability of one data record

- Impact of the replication strategy: UA(1,1)/UA(n,k)



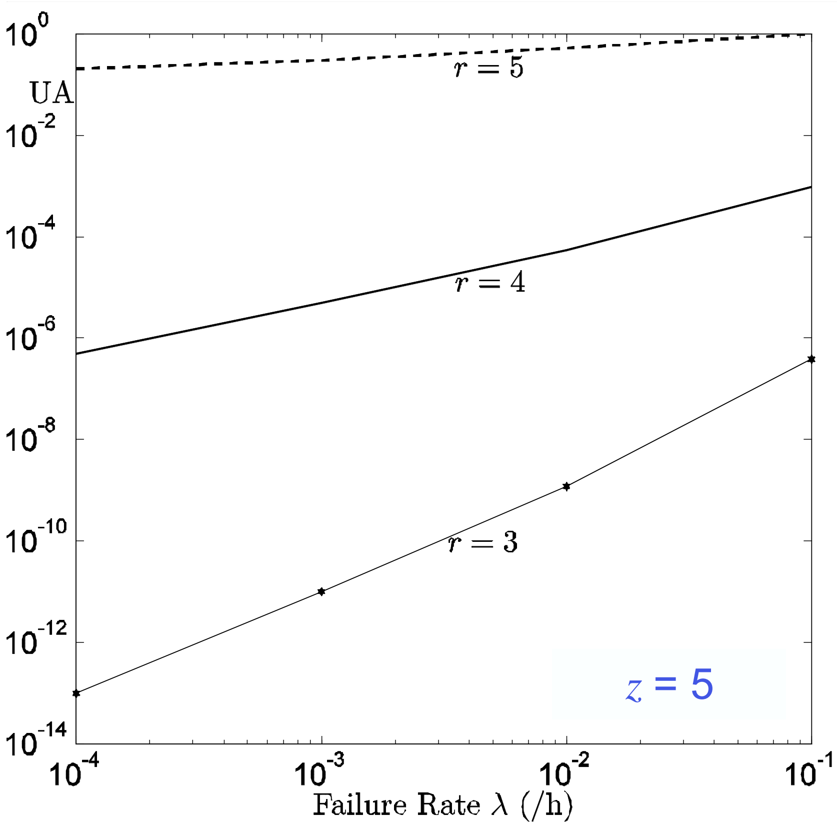
Exponential C2C encounters, c=100



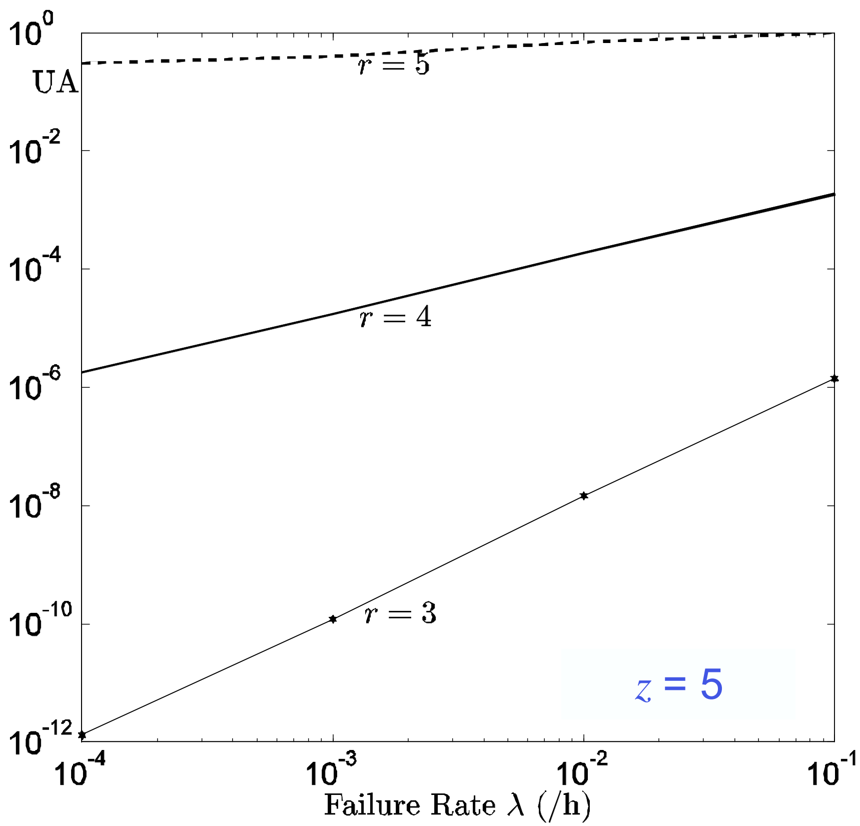
Pareto C2C encounters, c=100

VBB Unavailability

- Loss of multiple records
  - r among the last z generated records are needed to analyze what happened when an accident occur

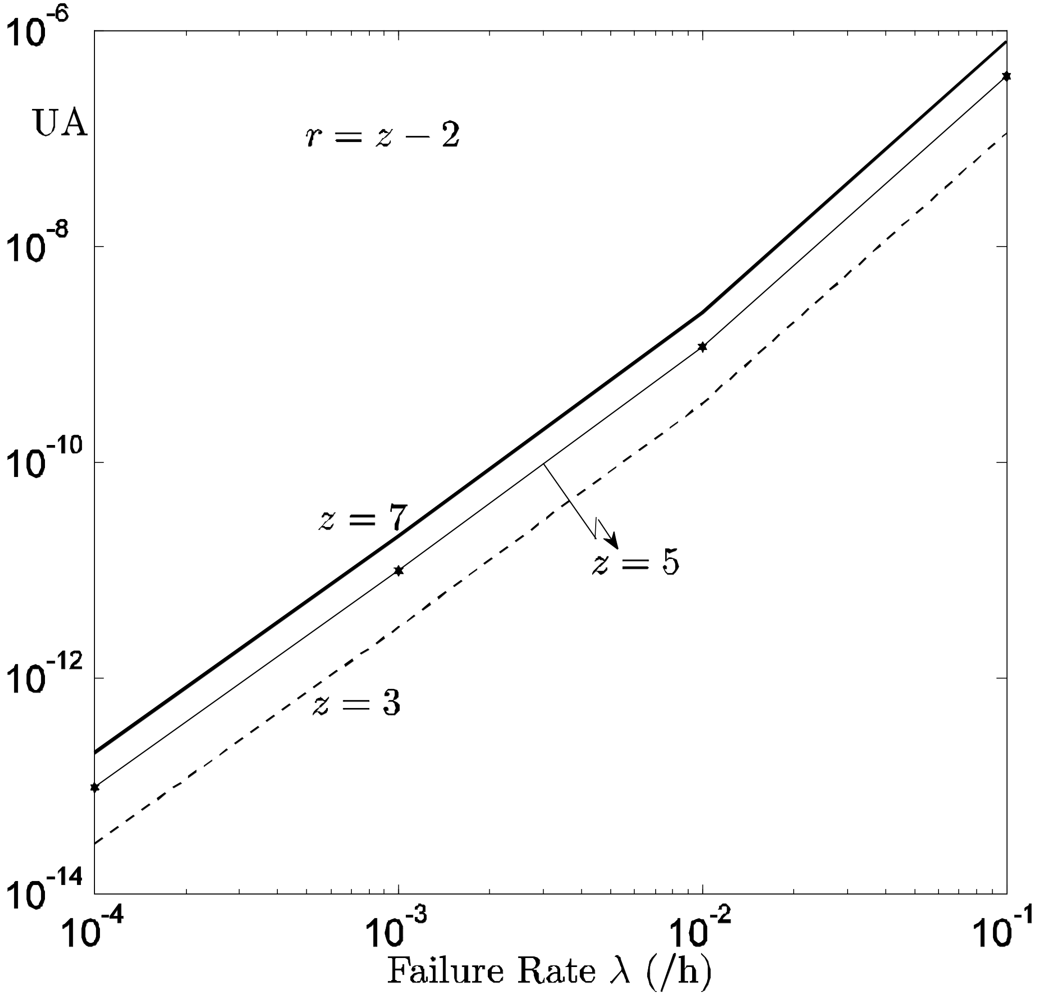


Exponential C2C encounters



Pareto C2C encounters

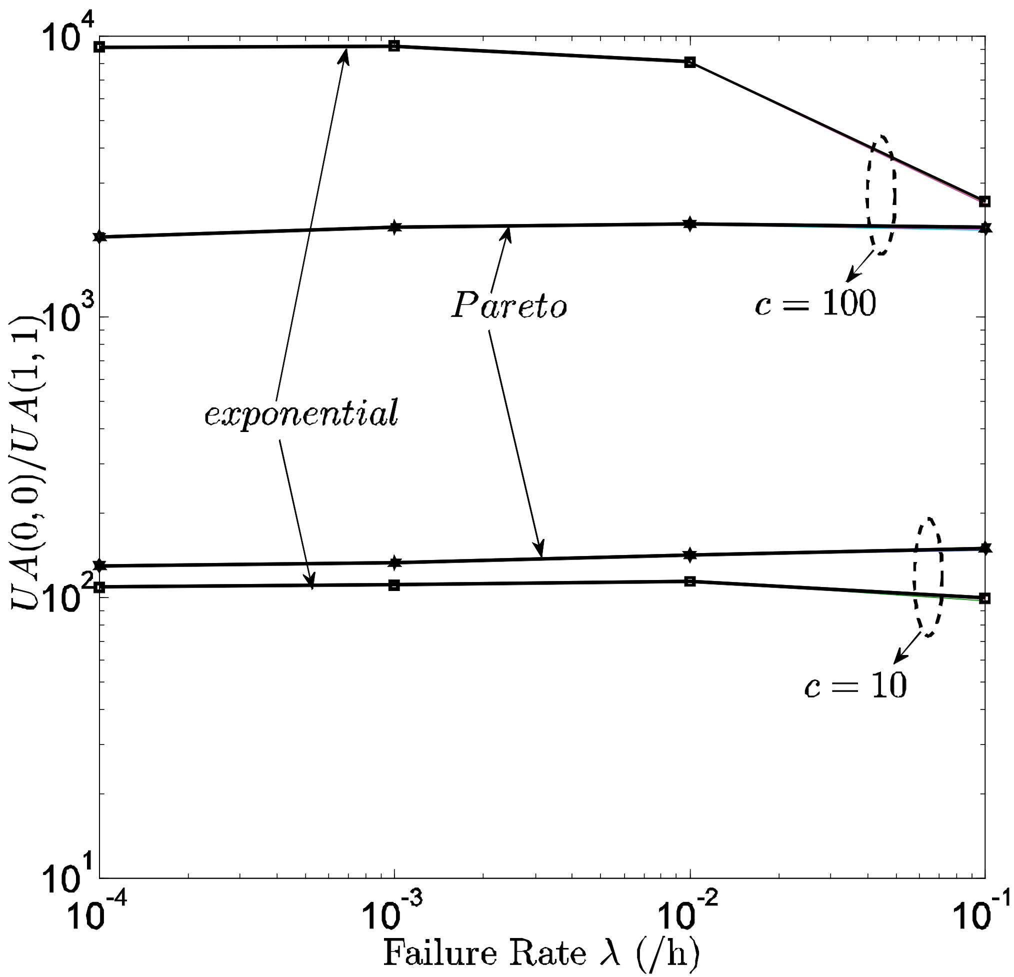
VBB Unavailability: impact of z



Exponential C2C encounters, c=100

VBB Unavailability

- Replication by duplication vs no replication



Virtual Black Box: Summary

- Combined modeling approach integrating dependability and connectivity dynamics

- Sensitivity analyses
  - Replication strategies under different mobility scenarios
    - Replication vs No replication: significant improvement
    - Duplication vs Erasure coding: same order of magnitude
  - Exponential vs Pareto distributed C2C encounters
    - Unavailability estimation may differ slightly (*a few times*) depending on the connectivity ratio and the failure rate

- Other applications:
  - platooning