Laboratoire Bordelais de Recherche en Informatique

Distributed algorithms in a (highly) dynamic context

S. Chaumette
serge.chaumette@labri.fr

LaBRI, Université Bordeaux 1

Laboratoire Bordelais de Recherche en Informatique

Based on

Laboratoire Bordelais de Recherche en Informatique

Outline

- Secured fleets of autonomous communicating mobile terminals
- Dynamic graphs and (secured) fleets of autonomous communicating mobile terminals
- The relationship of hardware design and security
- Example applications

Laboratoire Bordelais de Recherche en Informatique

Secured fleets of autonomous communicating mobile terminals

Laboratoire Bordelais de Recherche en Informatique

Outline

- Context
- Current approaches
- Real life
- Our approach, our target platforms

Laboratoire Bordelais de Recherche en Informatique

Outline

- Context
- Current approaches
- Real life
- Our approach, our target platforms

Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Context]

Laboratoire Bordelais de Recherche en Informatique

Goals and research topics of the Muse research group at LaBRI

Contribute to the definition and development of supporting middleware, tools and mechanisms formally validated that make it possible to take advantage of the resources (static or mobile) connected to the network (wired or wireless) and to develop applications on top of these resources.

Target systems

Secured fleets of autonomous communicating mobile terminals

Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Context]

Laboratoire Bordelais de Recherche en Informatique

We target real world networks

Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Context]

Laboratoire Bordelais de Recherche en Informatique

Nodes can move/appear/disappear

[Context]

Laboratoire Bordelais de Recherche en Informatique

Nodes can move/appear/disappear

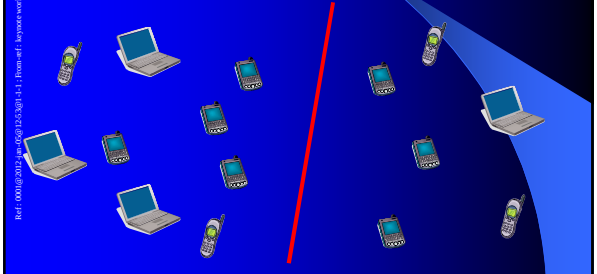
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Context]

Laboratoire Bordelais de Recherche en Informatique

The network can become disconnected



Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Context]

Laboratoire Bordelais de Recherche en Informatique

Summary of context and consequences

- (really) mobile Ad-hoc Networks (MANets)
  - → beyond Delay/Disruptive Tolerant Networks (DTN)

➔ High instability
- ➔ Very limited neighbourhood relationship
  - ➔ No communication guarantee
  - ➔ Routing is not a solution
  - ➔ Brute flooding is not a sufficient solution

➔ Users are most of the time not known in advance
- ➔ Unsecure boundaries

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

Laboratoire Bordelais de Recherche en Informatique

Outline

- Context
- Current approaches
- Real life
- Our approach, our target platforms
- Associated models
- Example applications

Laboratoire Bordelais de Recherche en Informatique

Current approaches

Applications have a **global** vision/knowledge

middleware

Laboratoire Bordelais de Recherche en Informatique

Current approaches

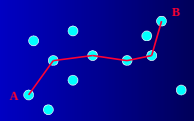
- Their goal is to hide the u… aspect by providing (c… ng to provide):
  - Routing
  - Sync… aranteed) communications

STOP TALKING ABOUT ROUTING!!!!!!!!!!!!
(in this precise context)

Laboratoire Bordelais de Recherche en Informatique

The routing based approach

- Proactive
  - OLSR, DSDV
- Reactive
  - AODV, TORA, DSR



[Current approaches: their limitations]

Laboratoire Bordelais de Recherche en Informatique

Basic asumption

- At any time a route can be established between two mobile units of the network, i.e. the network is connected and virtually stable
- → classical applications can be used
- → classical security techniques can be used
  ex.: Certification Authority
  (the problem of keys distribution remains)

Laboratoire Bordelais de Recherche en Informatique

Outline

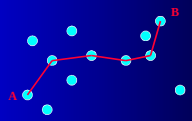
- Context
- Current approaches
- Real life
- Our approach, our target platforms

[Real life]

Laboratoire Bordelais de Recherche en Informatique

In the real life …

- Example:
  - Network of cars
  - Students on a campus
  - Tactical military networks
  - Crisis management
  - Home networking
  - …

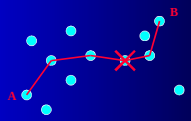


[Real life]

Laboratoire Bordelais de Recherche en Informatique

In the real life …

- Example:
  - Network of cars
  - Students on a campus
  - Tactical military networks
  - Crisis management
  - Home networking
  - …

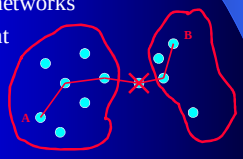


[Real life]

Laboratoire Bordelais de Recherche en Informatique

In the real life …

- Example:
  - Network of cars
  - Students on a campus
  - Tactical military networks
  - Crisis management
  - Home networking
  - …



Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

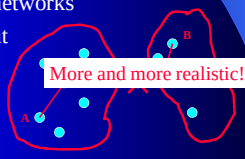
[Real life]

Laboratoire Bordelais de Recherche en Informatique

In the real life …

- Example:
  - Network of cars
  - Students on a campus
  - Tactical military networks
  - Crisis management
  - Home networking
  - …

More and more realistic!



Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Real life]

Laboratoire Bordelais de Recherche en Informatique

The nature of the network changes

➔ The nature of applications changes
  – group/community based, dynamic, …
    ➔ the Internet of Things

➔ The management of security changes

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Real life]

Laboratoire Bordelais de Recherche en Informatique

Paradigm shift for applications

How many people are there ?

Are there many people ?
(or approximate number)

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Real life]

Laboratoire Bordelais de Recherche en Informatique

Impact on applications

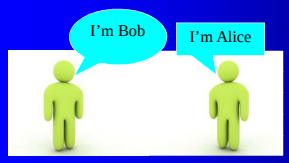
- The objectives must be lowered because of high instability
- Examples:
  - counting → lower bound
  - covering tree→ covering forest
- But .. this is real life ☺

Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010

[Real life]

Laboratoire Bordelais de Recherche en Informatique

Paradigm shift for security



Share keys, authenticate

Recognize
- individually
- group/topic based

Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010

[Real life]

Laboratoire Bordelais de Recherche en Informatique

Impact on security

- The objectives must be lowered because of unsecure boudaries
- Examples:
  - Entity based keyes → group/topic based keyes
  - authenticate → recognize
- But once again … this is real life ☺

Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010

Laboratoire Bordelais de Recherche en Informatique

Outline

- Context
- Current approaches
- Real life
- Our approach, our target platforms

Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010

Laboratoire Bordelais de Recherche en Informatique

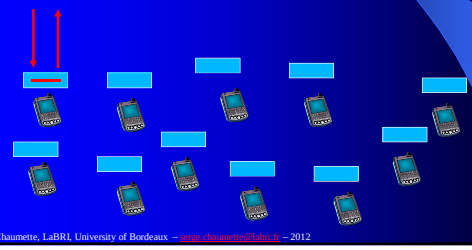
Our approach

The middleware is never seen as something global
➔ the applications interact locally

Laboratoire Bordelais de Recherche en Informatique

Applications management
Local – local primitives

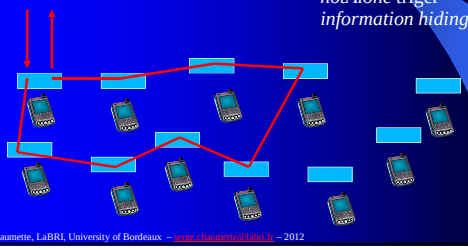
Local impact
Local computation
Examples: one way communication



Laboratoire Bordelais de Recherche en Informatique

Applications management
Local – remote primitives

Local impact
Distributed/remote computation
Examples: *haveBeenHeard* triger
notAlone triger
information hiding



Laboratoire Bordelais de Recherche en Informatique

Security management

[Our approach]

Laboratoire Bordelais de Recherche en Informatique

A vertical approach

application

Distributed algorithms (P2P), specialized languages

Middleware

- P2P communication
- hardware heterogeneity
- management
  - . adaptation to the environnement
  - . code generation

hardware

- unstability
  - . of the network
  - . of the drones
- security
  - . based on smart cards
  - . wired dedicated features
- adaptation
  - - security, radio, etc.

+ validation, modelisation and verification

Ref : 0001@2012-jan-05@12-53@1-1-1 ; from ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Our approach]

Laboratoire Bordelais de Recherche en Informatique

A tentative taxonomy

- Wireless Networks
  - Ad hoc
    - Mobile
      - MANets
      - VANets
      - UAVNets
      - SensorNets
      - MEMSNets
    - Static
      - SensorNets
      - MEMSNets
  - Infrastructured

Ref : 0001@2012-jan-05@12-53@1-1-1 ; from ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Our approach]

Laboratoire Bordelais de Recherche en Informatique

Our target systems

Secured fleets of autonomous communicating mobile terminals

- Fleets of mobile phones
  - – 100 Android phones
- Fleets of robots
  - – 10 prototypes being built → fleet of 200
- Fleets of UAVs
  - – Fly-n-Sense + DGA (French army)

Ref : 0001@2012-jan-05@12-53@1-1-1 ; from ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Our approach]

Laboratoire Bordelais de Recherche en Informatique

Fleet of Android mobile phones

Ref : 0001@2012-jan-05@12-53@1-1-1 ; from ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Our approach]

Laboratoire Bordelais de Recherche en Informatique

Underlying constraints

- Behavior of the fleet members
  - unpredictable mobility
  - unpredictable volatility
- Possible controls of the fleet members
  - none

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Our approach]

Laboratoire Bordelais de Recherche en Informatique

Fleet of robots

- This work is being carried out with Olivier Ly and Hugo Gimbert
  - Mobility
  - XBee Communication
  - Localization (?)
  - Infra-red targeting (?)

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Our approach]

Laboratoire Bordelais de Recherche en Informatique

Underlying constraints

- Behavior of the fleet members
  - partially predictable mobility
  - unpredictable volatility
- Possible controls of the fleet members
  - partial mobility control

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Our approach]

Laboratoire Bordelais de Recherche en Informatique

Fleet of UAVs

- Collaboration
  - Fly-n-Sens, IMS, ENAC
    - SYMM project labeled by the world competitivity cluster Aerospace Valley
  - DGA (french Army)

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Our approach]

Laboratoire Bordelais de Recherche en Informatique

Underlying constraints

- Behavior of the fleet members
  - partially predictable mobility
  - unpredictable volatility
- Possible control of the fleet members
  - (almost) total mobility control

[Our approach]

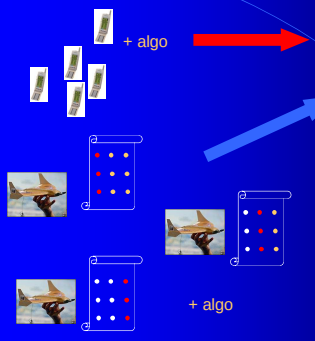
Laboratoire Bordelais de Recherche en Informatique

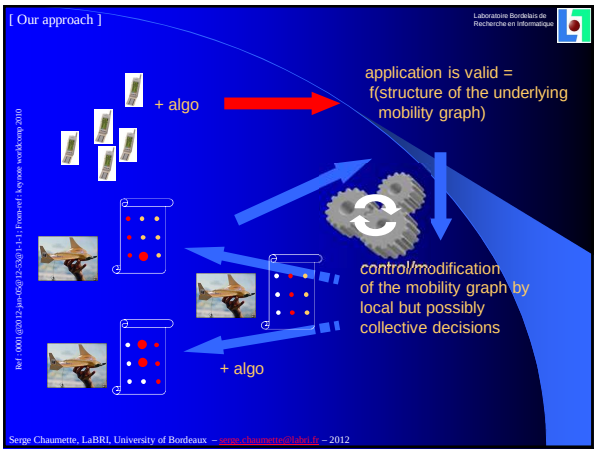
[Our approach]

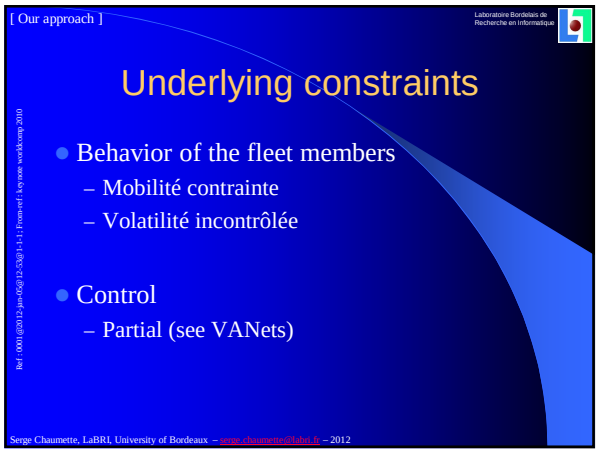
Laboratoire Bordelais de Recherche en Informatique

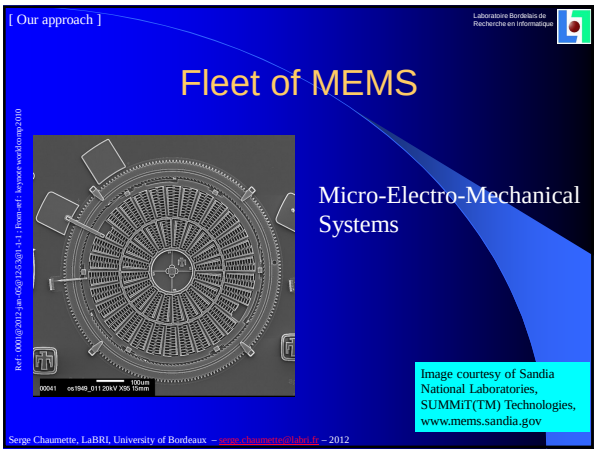
[Our approach]

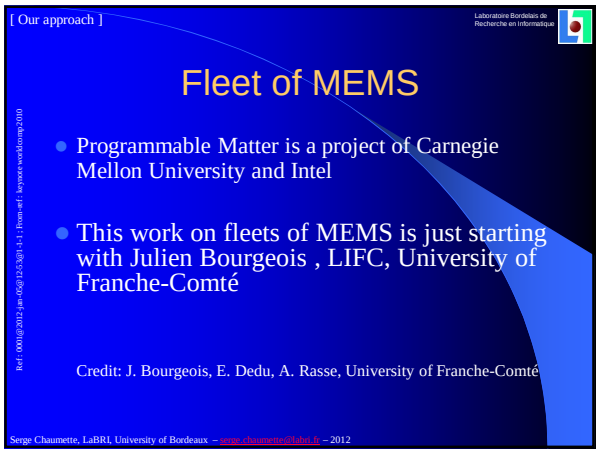
Laboratoire Bordelais de Recherche en Informatique




[Our approach]
Laboratoire Bordelais de Recherche en Informatique
+ algo
application is valid = f(structure of the underlying mobility graph)
control/modification of the mobility graph by local but possibly collective decisions
+ algo
Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Our approach]
Laboratoire Bordelais de Recherche en Informatique
Underlying constraints
Behavior of the fleet members
– Mobilité contrainte
– Volatilité incontrôlée
Control
– Partial (see VANets)
Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Our approach]
Laboratoire Bordelais de Recherche en Informatique
Fleet of MEMS
Micro-Electro-Mechanical Systems
Image courtesy of Sandia National Laboratories, SUMMiT(TM) Technologies, www.mems.sandia.gov
Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Our approach]
Laboratoire Bordelais de Recherche en Informatique
Fleet of MEMS
Programmable Matter is a project of Carnegie Mellon University and Intel
This work on fleets of MEMS is just starting with Julien Bourgeois , LIFC, University of Franche-Comté
Credit: J. Bourgeois, E. Dedu, A. Rasse, University of Franche-Comté
Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Our approach]

Laboratoire Bordelais de Recherche en Informatique

Main problems

Volatility (unstability)
- of terminals
- of the network

Redesign of algorithms (no routing, no global knowledge, disconnected network, etc.)

Security is a major problem

Using Smart Cards

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

Laboratoire Bordelais de Recherche en Informatique

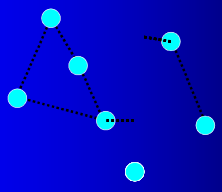
Outline

- Secured fleets of autonomous communicating mobile terminals
- Dynamic graphs and (secured) fleets of autonomous communicating mobile terminals
- The relationship of hardware design and security
- Example applications

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

Laboratoire Bordelais de Recherche en Informatique

Dynamic graphs and (secured) fleets of autonomous communicating mobile terminals



Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Approach]

Laboratoire Bordelais de Recherche en Informatique

Approach

- Local computation

graph relabeling

- (other approach: CCS/CBP (Milner, Prasad) like models - work in progress -)

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Graph relabeling]

Laboratoire Bordelais de Recherche en Informatique

Graph relabeling

- Static graphs → Sirocco-2000-2-2
- Dynamic, évolutive graphs → Sirocco-2000-3-55-7
- The dynamic aspect must be taken into account by the applications
  - Example of the spanning forest → PhD-AC-2007-11-11

Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Relabeling over graphs]

Laboratoire Bordelais de Recherche en Informatique

Relabeling over graphs

- Static graphs
  - →see [Litovsky, Metivier, Sopena 1999]

- extension to dynamic graphs
  - →see [Casteigts, Chaumette, Ferreira 2009]

Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Relabeling over static graphs]

Laboratoire Bordelais de Recherche en Informatique

Relabeling over static graphs

- Local computation in static graphs
  - A node can only interact with a direct neighbor
  - Nodes/communication links are static
- Example :
  - the rule
    will eventually make all the nodes red

More complex example: an algorithm that creates a spanning tree

→ I. Litovsky, Y. Metivier, and E. Sopena. Graph relabelling systems and distributed algorithms. In World Scientic Publishing, editor, Handbook of graph grammars and computing by graph transformation, volume III, Eds.

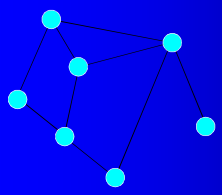
Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Relabeling over static graphs / the spanning tree example]

Laboratoire Bordelais de Recherche en Informatique

The spanning tree example

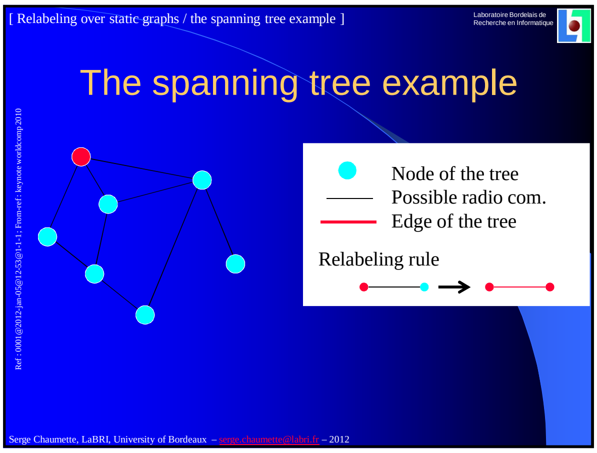


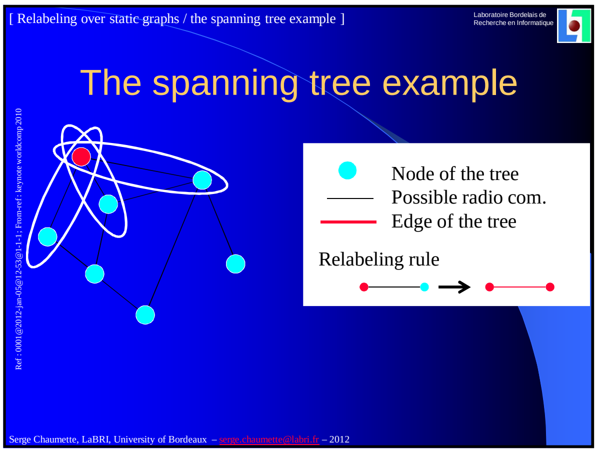
Node of the tree
Possible radio com.
Edge of the tree

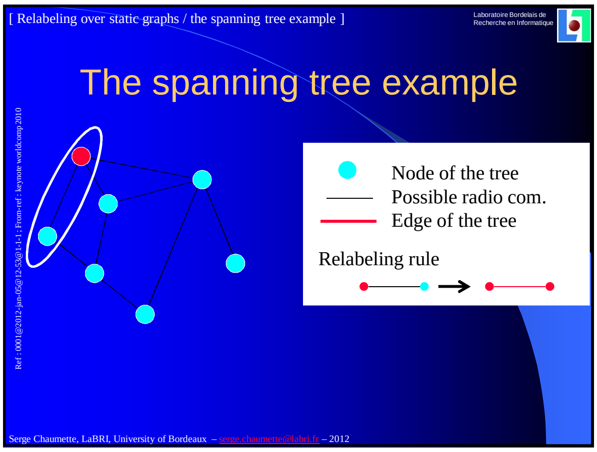
Relabeling rule

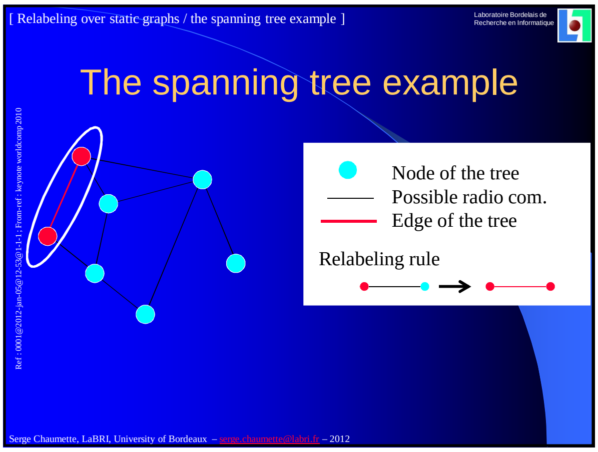
Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010

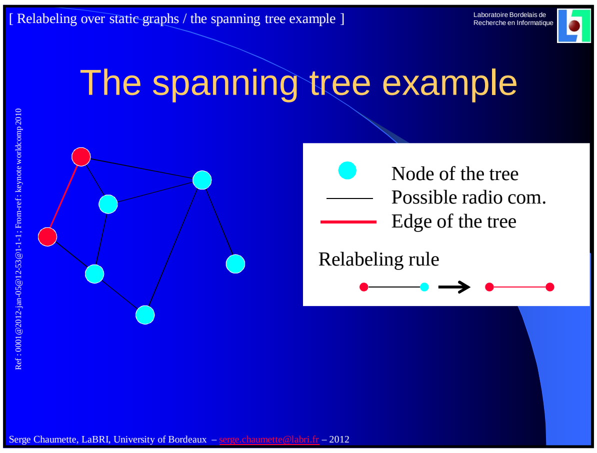
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

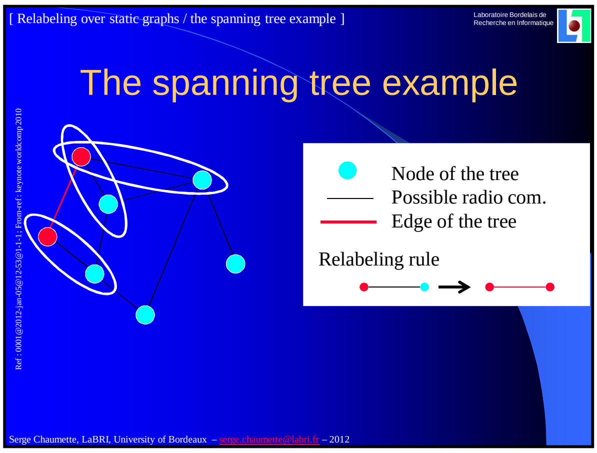

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

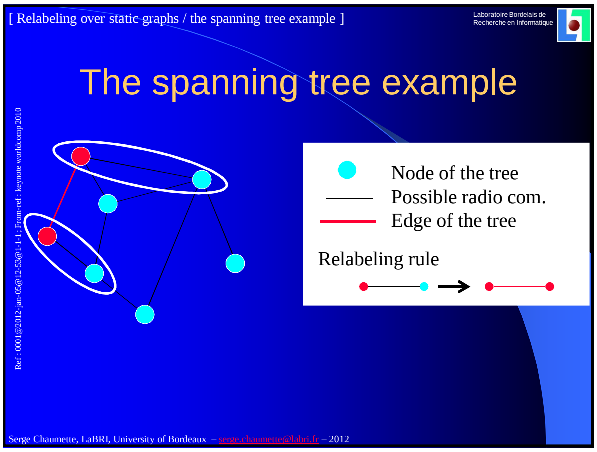

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

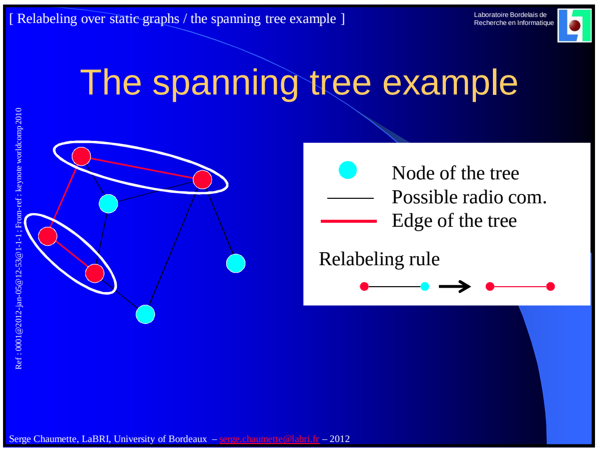

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

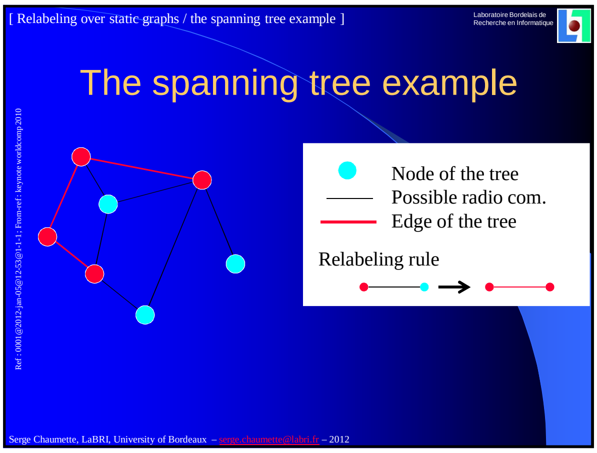

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

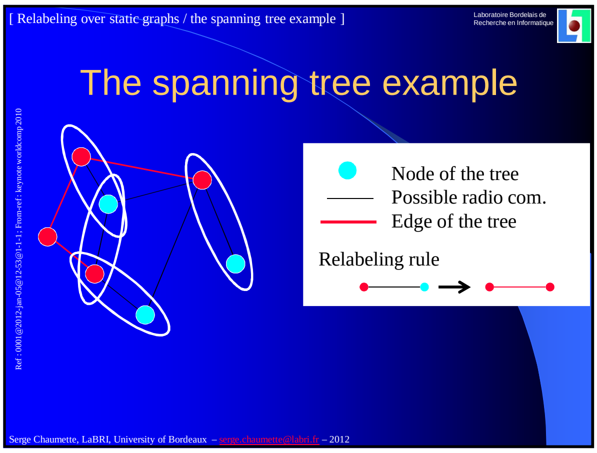

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

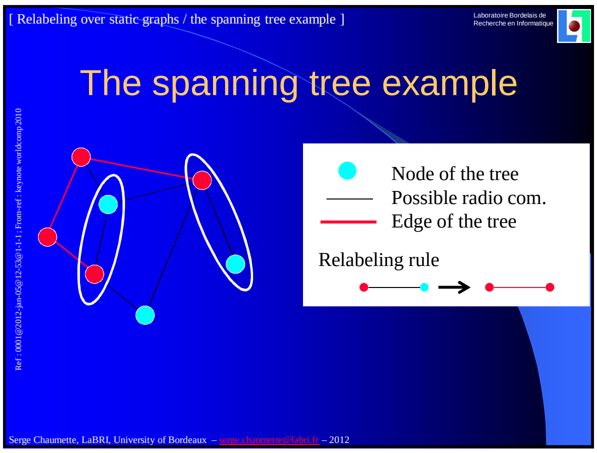

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

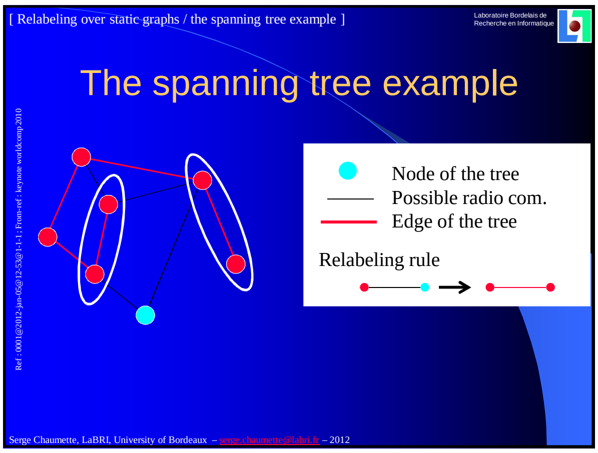

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

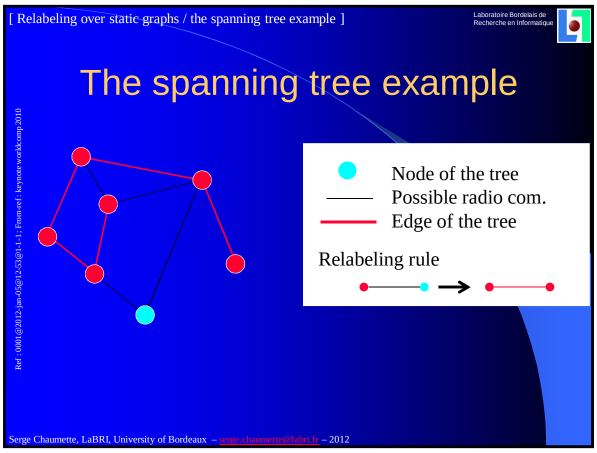

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

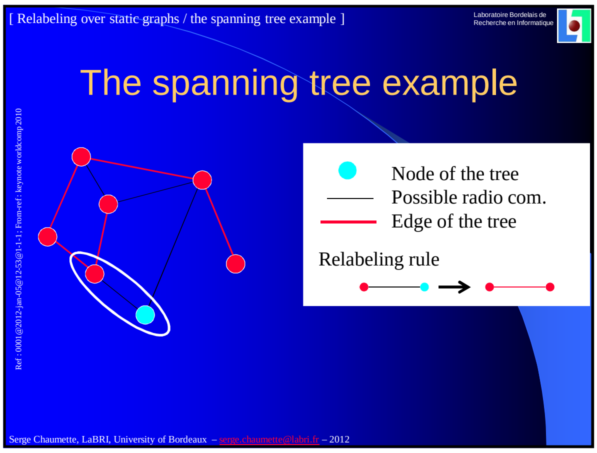

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

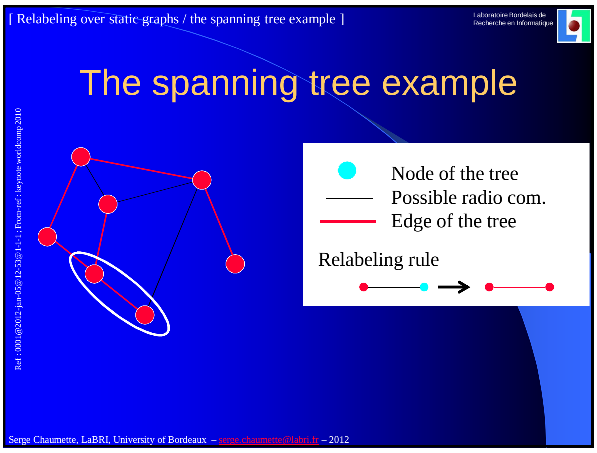

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

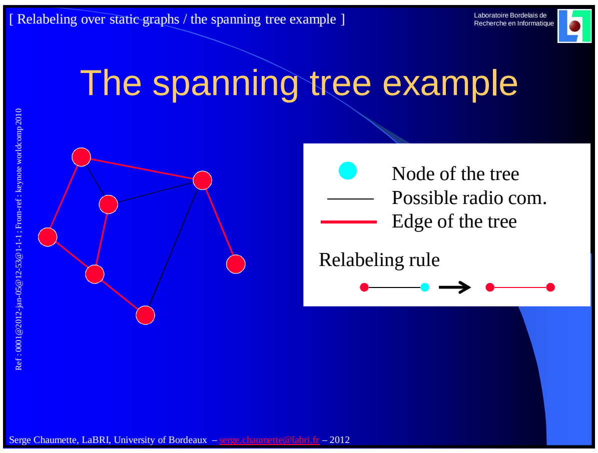

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

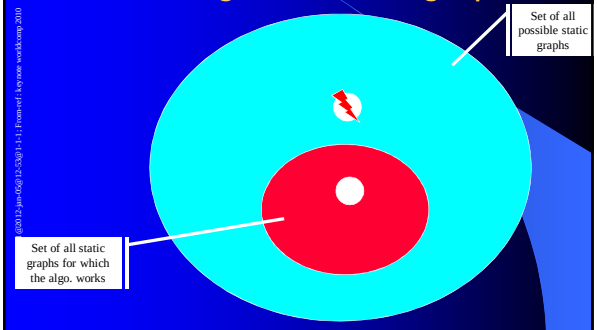

[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Relabeling over static graphs / the spanning tree example]
Laboratoire Bordelais de Recherche en Informatique
The spanning tree example
Node of the tree
Possible radio com.
Edge of the tree
Relabeling rule
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

[Relabeling over static graphs]

Laboratoire Bordelais de Recherche en Informatique

Relabeling over static graphs



Ref : 001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Relabeling over dynamic graphs]

Laboratoire Bordelais de Recherche en Informatique

Relabeling over dynamic graphs

- Relabeling rules as for static graphs

- Management of appearing vertices

- Management of disappearing vertices

Ref : 001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Relabeling over dynamic graphs]

Laboratoire Bordelais de Recherche en Informatique

Model

- Local computation in dynamic graphs
  - A node can only interact with a direct neighbor
  - Nodes/com.links can appear/disappear at any time
- Example :
  - the rule

will not necessarily make all the nodes red

More complex example: an algorithm that maintains a spanning forest with nodes arriving and leaving at any time and with unstable communication links

→ Arnaud Casteigts, Serge Chaumette, Afonso Ferreira: Characterizing Topological Assumptions of Distributed Algorithms in Dynamic Networks. SIROCCO 2009: 126-140

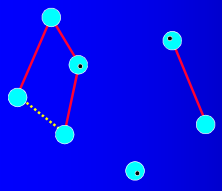
http://hal.archives-ouvertes.fr/docs/00/37/67/01/PDF/RR-1457-09.pdf

Ref : 001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

[Relabeling over dynamic graphs / The spanning forest example]

Laboratoire Bordelais de Recherche en Informatique

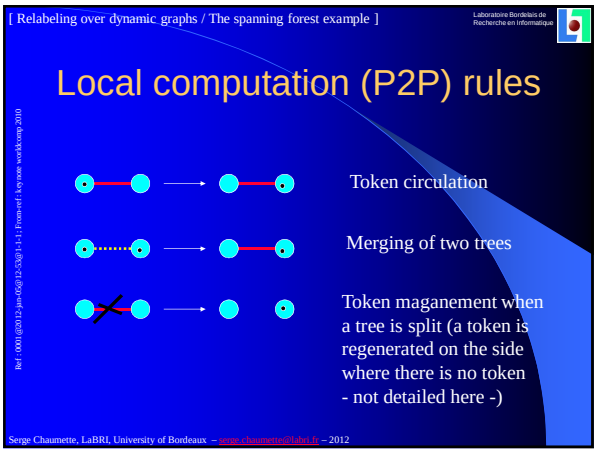
The spanning forest example

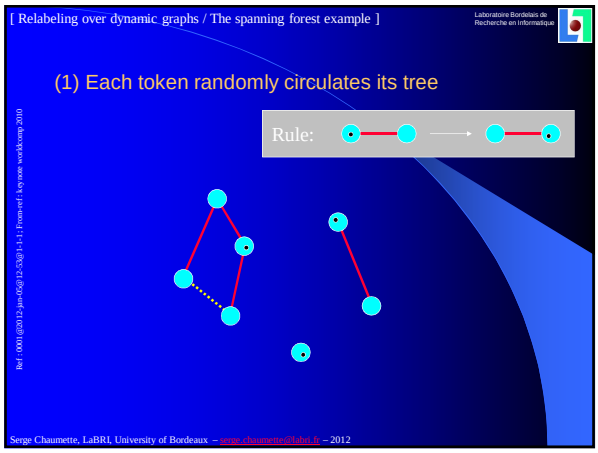


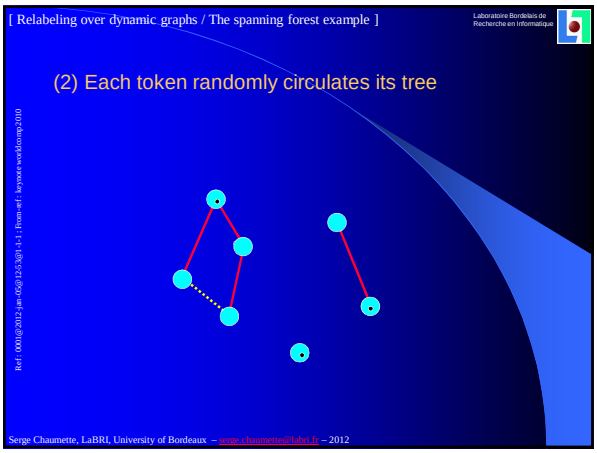
Node of one of the trees
Token
Possible radio com.
Edge of one of the trees

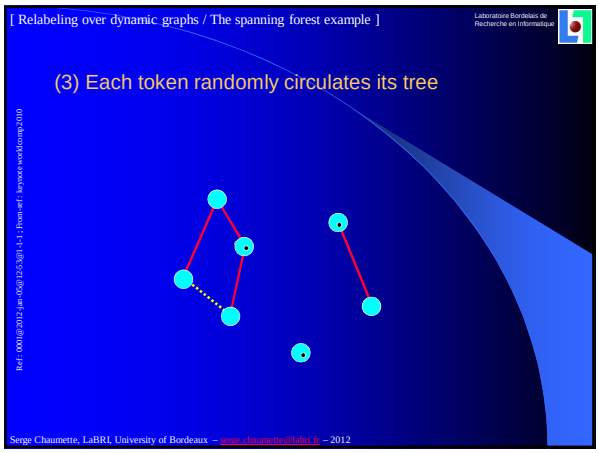
→ At any time each node is inside one and only one tree (that also has one and only one token)

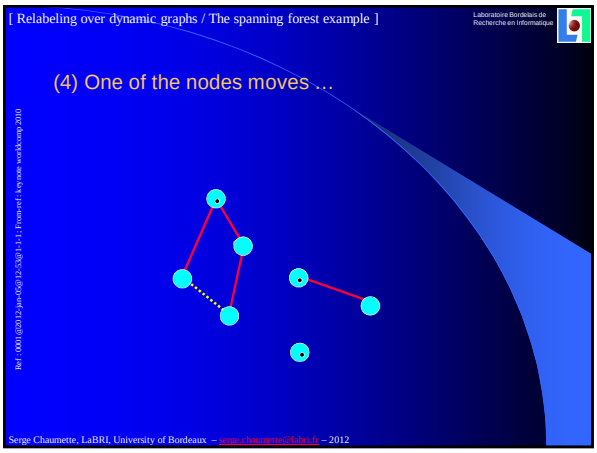
Ref : 001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010

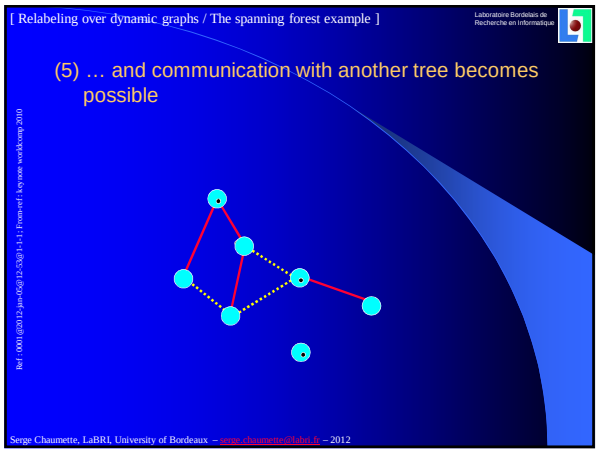

[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
Local computation (P2P) rules
Token circulation
Merging of two trees
Token maganement when a tree is split (a token is regenerated on the side where there is no token - not detailed here -)
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

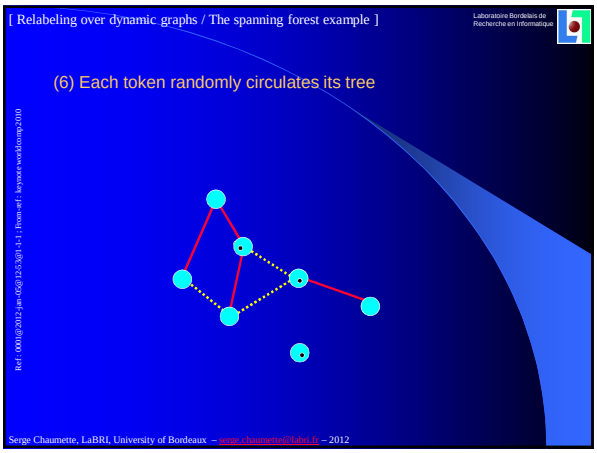

[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
(1) Each token randomly circulates its tree
Rule:
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

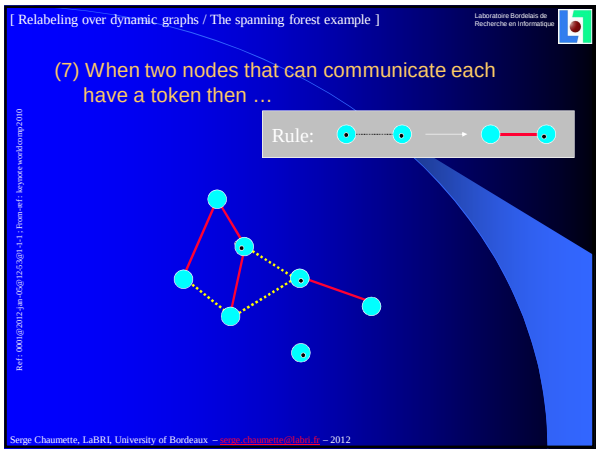

[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
(2) Each token randomly circulates its tree
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

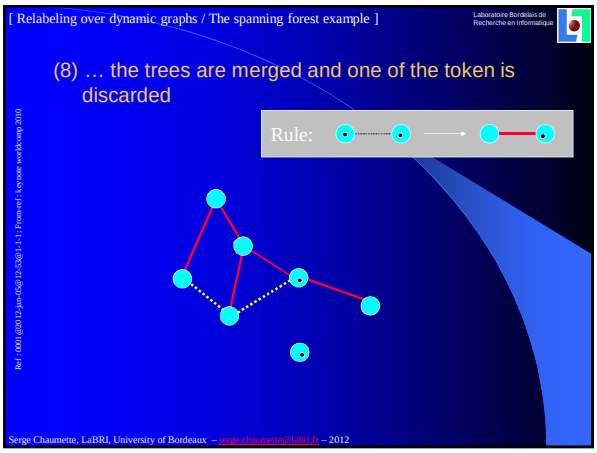

[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
(3) Each token randomly circulates its tree
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

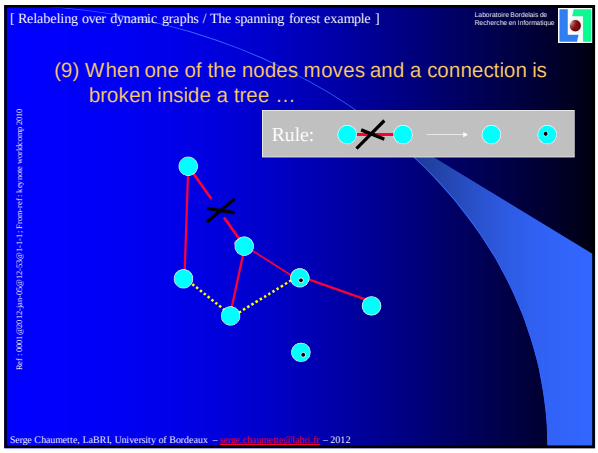

[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
(4) One of the nodes moves …
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

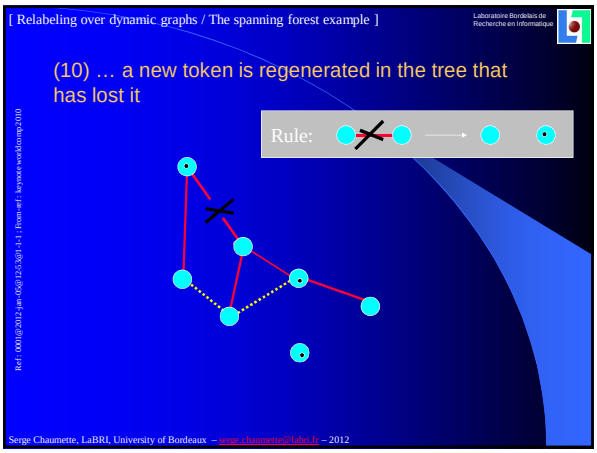

[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
(5) … and communication with another tree becomes possible
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

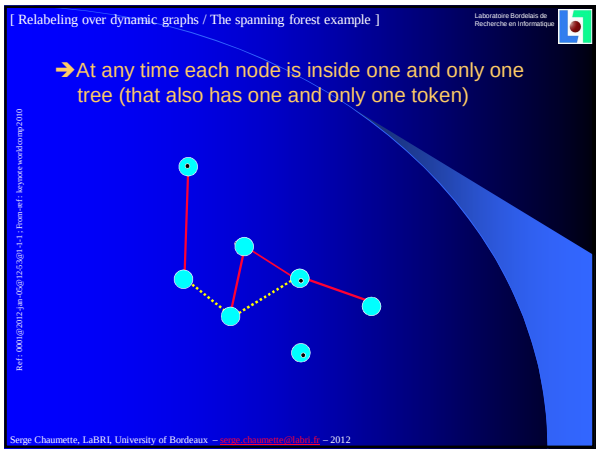

[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
(6) Each token randomly circulates its tree
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
(7) When two nodes that can communicate each have a token then …
Rule:
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
(8) … the trees are merged and one of the token is discarded
Rule:
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
(9) When one of the nodes moves and a connection is broken inside a tree …
Rule:
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
(10) … a new token is regenerated in the tree that has lost it
Rule:
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Relabeling over dynamic graphs / The spanning forest example]
Laboratoire Bordelais de Recherche en Informatique
➔At any time each node is inside one and only one tree (that also has one and only one token)
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

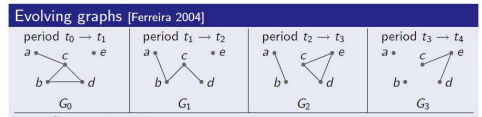
Evolving graphs

Laboratoire Bordelais de Recherche en Informatique

Formalism to represent dynamic topology

Evolving graphs [Ferreira 2004]

period $t_0 \rightarrow t_1$ | period $t_1 \rightarrow t_2$ | period $t_2 \rightarrow t_3$ | period $t_3 \rightarrow t_4$

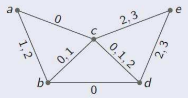


G_0 G_1 G_2 G_3

$\mathcal{S}_T = t_0, t_1, t_2, t_3, t_4$
$\mathcal{S}_G = G_0, G_1, G_2, G_3$
$G = \bigcup_{G_i \in \mathcal{S}_G} =$ 

$\} \; \mathcal{G} = (G, \mathcal{S}_G, \mathcal{S}_T)$
is the corresponding *Evolving Graph*.

↓ graphical representation ↓



A.Casteigts, S.Chaumette, A.Ferreira
Characterizing Topological Assumptions of Dist. Algo. in Dynamic Networks 5 / 15

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012 Slide from Sirocco 2009

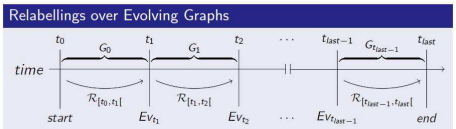
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkomp 2010

DAGRS over evolving graphs

Laboratoire Bordelais de Recherche en Informatique

Combination

Relabellings over Evolving Graphs



An execution is an alternated sequence of relabellings and topological events:
$X = \mathcal{R}_{\mathcal{A}_{[t_{last-1},t_{last}[}} \circ Event_{t_{last-1}} \circ .. \circ Event_{t_1} \circ \mathcal{R}_{\mathcal{A}_{[t_1-1,t_1[}} \circ .. \circ Event_{t_1} \circ \mathcal{R}_{\mathcal{A}_{[t_0,t_1[}}(G_0)$

We note $\mathcal{X}_{\mathcal{A}/\mathcal{G}}$ the set of all possible execution sequences of an algorithm $\mathcal{A}$ over an evolving graph $\mathcal{G}$

Topology-related necessary condition: $\neg\mathcal{C}_{\mathcal{N}}(\mathcal{G}) \implies \nexists X \in \mathcal{X}_{\mathcal{A}/\mathcal{G}} \mid success.$
Topology-related sufficient condition: $\mathcal{C}_{\mathcal{S}}(\mathcal{G}) \implies \forall X$ in $\mathcal{X}_{\mathcal{A}/\mathcal{G}}$, *success*.

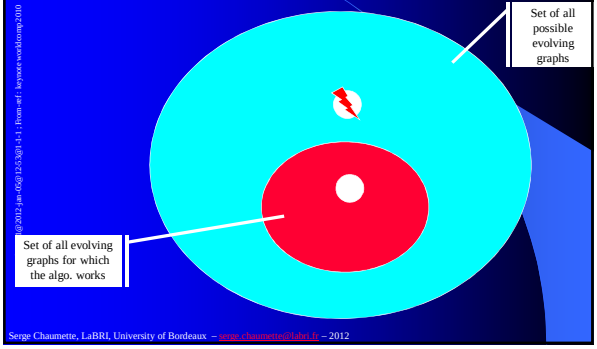
A.Casteigts, S.Chaumette, A.Ferreira
Characterizing Topological Assumptions of Dist. Algo. in Dynamic Networks 6 / 15

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012 Slide from Sirocco 2009

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkomp 2010

DAGRS over evolving graphs

Laboratoire Bordelais de Recherche en Informatique



Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

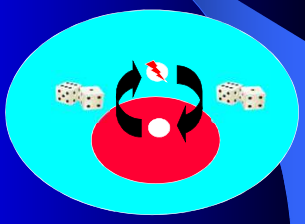
Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkomp 2010

Fleet of mobile phone

Laboratoire Bordelais de Recherche en Informatique

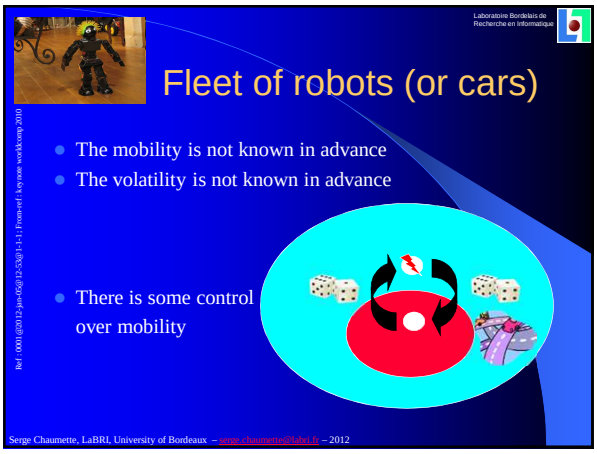
- The mobility is not known in advance
- The volatility is not known in advance

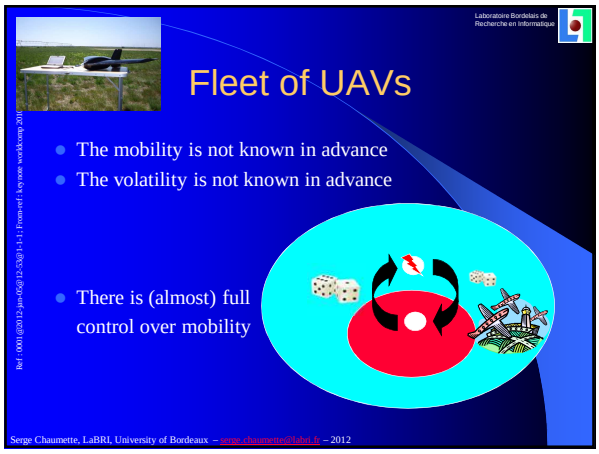
- There is no control over mobility



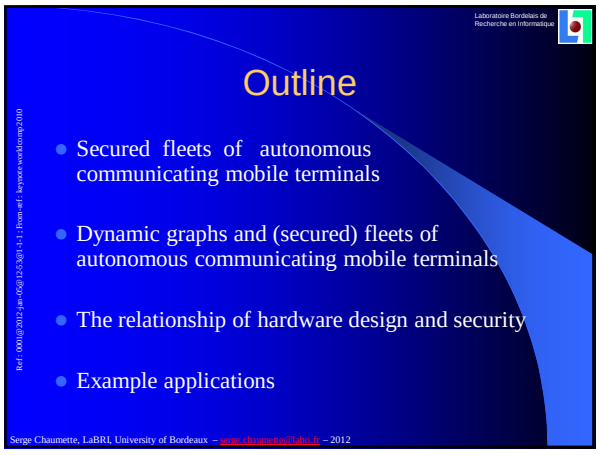
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

Ref : 0001@2012-jan-05@12-53@1-1-1 ; From ref : keynote workkomp 2010


Laboratoire Bordelais de Recherche en Informatique
Fleet of robots (or cars)
The mobility is not known in advance
The volatility is not known in advance
There is some control over mobility
Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


Laboratoire Bordelais de Recherche en Informatique
Fleet of UAVs
The mobility is not known in advance
The volatility is not known in advance
There is (almost) full control over mobility
Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


Laboratoire Bordelais de Recherche en Informatique
CCS-bx [work in progress]
Synchronous communication
Asynchronus communication
Message loss
Delayed reception when broadcasting
Mobility of nodes and messages
Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


Laboratoire Bordelais de Recherche en Informatique
Outline
Secured fleets of autonomous communicating mobile terminals
Dynamic graphs and (secured) fleets of autonomous communicating mobile terminals
The relationship of hardware design and security
Example applications
Ref : 0001@2012-jan-05@12-53@1-1-1 : From ref : keynote workkcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

Laboratoire Bordelais de Recherche en Informatique

The relationship of hardware design and security

Laboratoire Bordelais de Recherche en Informatique

Outline

- Identities
- Components interconnections
- Add-ons

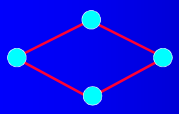
Laboratoire Bordelais de Recherche en Informatique

Identities

- Identities (even if not avaibale at user level) are usefull to solve some effective problems:
  - election
  - routing
  - …

Laboratoire Bordelais de Recherche en Informatique

Why they cannot be generated



There is no way to make any différence between any two nodes.

Any algorithm will be executed the same way and will thus produce exactly the same values on each node

Laboratoire Bordelais de Recherche en Informatique

« The » reference paper

Dana Angluin
Local and global properties in networks of processors
(Extended Abstract)
Proceedings of the twelfth annual ACM symposium on Theory of computing, p.82-93, April 28-30, 1980, Los Angeles, California, United States

Laboratoire Bordelais de Recherche en Informatique

Hardware approaches

- Crypto based approach
  - Based on RNGs
    - are TRGNS really available in mobile devices?
    - probabilistic result
- TPM based
  - Additional cost (hard)
  - Expensive to secure (personnalization)
  - How to link it to the rest of the hardware ?
- Physical Unclonable Function based (see *'project proposal'* later) as a solution ?

Laboratoire Bordelais de Recherche en Informatique

Components interconnections

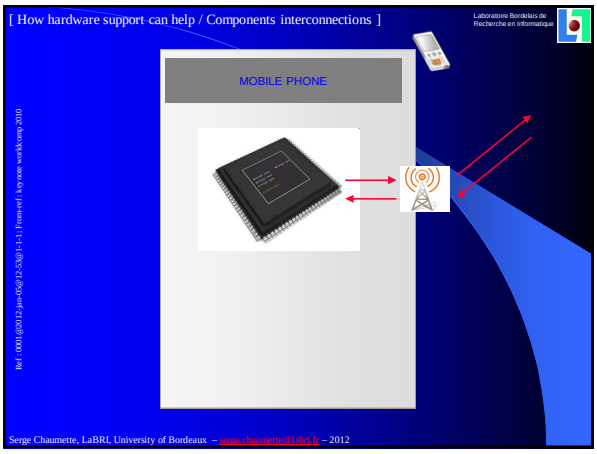
Laboratoire Bordelais de Recherche en Informatique

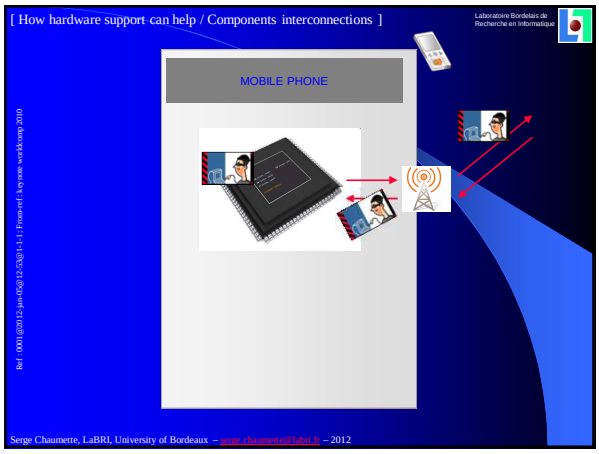
From an application perspective

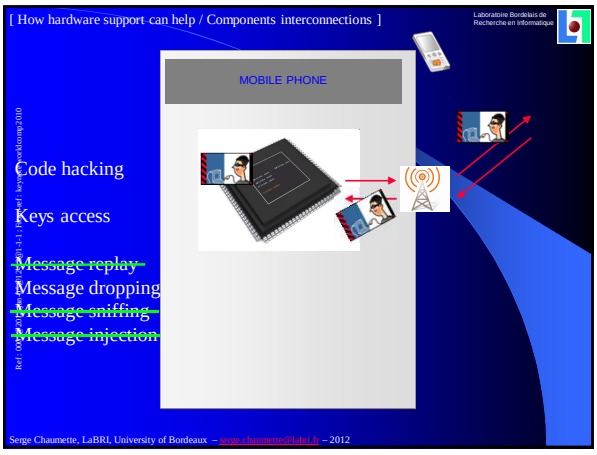
- Non functional properties
  - Secure the application itself
  - Secure secret/public keys
- Functional properties

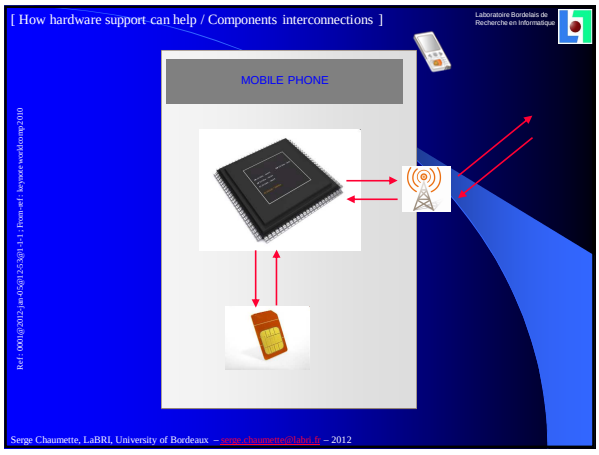
→What is the best you can do to send a message ?

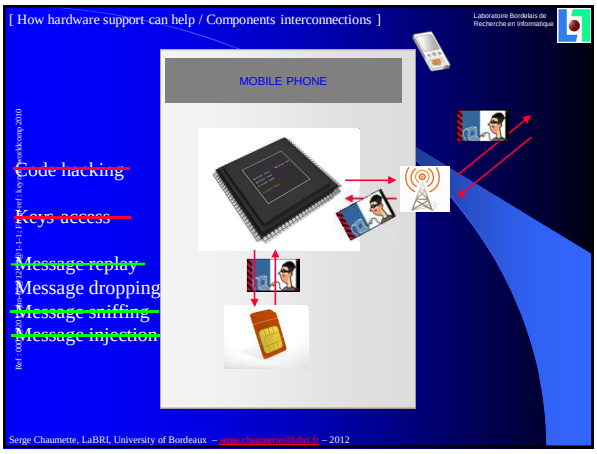
→ What is the best you can do to properly handle an incoming message ?

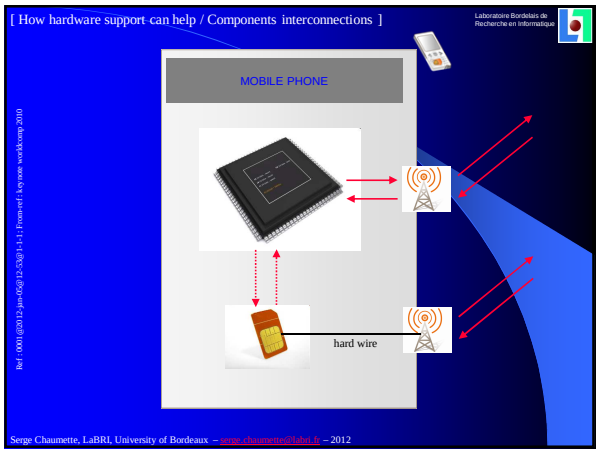

[How hardware support can help / Components interconnections]
Laboratoire Bordelais de Recherche en Informatique
MOBILE PHONE
Ref : 0001@2012-jan-05@12-53@1-1-1 From-ref : keynote wosdcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

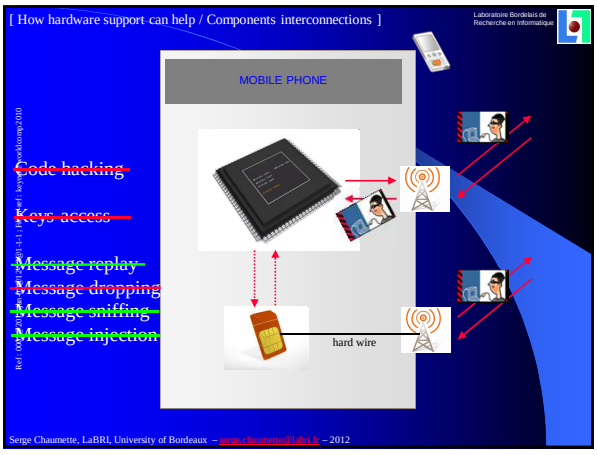

[How hardware support can help / Components interconnections]
Laboratoire Bordelais de Recherche en Informatique
MOBILE PHONE
Ref : 0001@2012-jan-05@12-53@1-1-1 From-ref : keynote wosdcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

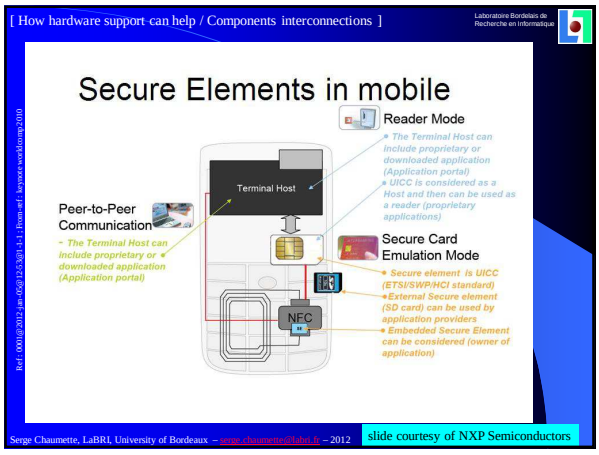

[How hardware support can help / Components interconnections]
Laboratoire Bordelais de Recherche en Informatique
MOBILE PHONE
Code hacking
Keys access
~~Message replay~~
Message dropping
~~Message sniffing~~
~~Message injection~~
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[How hardware support can help / Components interconnections]
Laboratoire Bordelais de Recherche en Informatique
MOBILE PHONE
Ref : 0001@2012-jan-05@12-53@1-1-1 From-ref : keynote wosdcomp 2010
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012

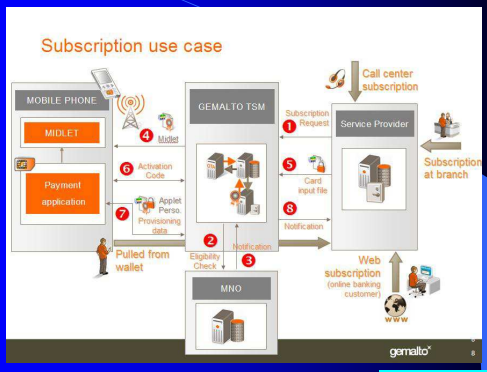

[How hardware support can help / Components interconnections]
Laboratoire Bordelais de Recherche en Informatique
MOBILE PHONE
Code hacking
Keys access
Message replay
Message dropping
Message sniffing
Message injection
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[How hardware support can help / Components interconnections]
Laboratoire Bordelais de Recherche en Informatique
MOBILE PHONE
hard wire
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[How hardware support can help / Components interconnections]
Laboratoire Bordelais de Recherche en Informatique
MOBILE PHONE
Code hacking
Keys access
Message replay
Message dropping
Message sniffing
Message injection
hard wire
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[How hardware support can help / Components interconnections]
Laboratoire Bordelais de Recherche en Informatique
Secure Elements in mobile
Reader Mode
The Terminal Host can include proprietary or downloaded application (Application portal)
UICC is considered as a Host and then can be used as a reader (proprietary applications)
Terminal Host
Peer-to-Peer Communication
The Terminal Host can include proprietary or downloaded application (Application portal)
Secure Card Emulation Mode
Secure element is UICC (ETSI/SWP/HCI standard)
External Secure element (SD card) can be used by application providers
Embedded Secure Element can be considered (owner of application)
NFC
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012
slide courtesy of NXP Semiconductors

Global impact



Slide courtesy of gemalto

[How hardware support can help / add-ons]

Add-ons

The case of NFC technology

- Phones hardly available (Nokia from 2011)
- Extra cost for (yet) little usage opportunities
- Responsibility of manufacturers for embedding untested (on a large scale) technology

➔ add-ons provide an on demand solution

[How hardware support can help / add-ons]

source tyfone.com

[How hardware support can help / add-ons]

source www.icarte.ca

Laboratoire Bordelais de Recherche en Informatique

Outline

- Secured fleets of autonomous communicating mobile terminals
- Dynamic graphs and (secured) fleets of autonomous communicating mobile terminals
- Example applications

Laboratoire Bordelais de Recherche en Informatique

Example applications (based on collaborations)

- With the industry
  - Gemalto, Thales, NXP, Oberthur, Orange, G&D
  - Verisign
  - Intelligere
  - Fly-n-Sense
  - …
- With gouvernemental bodies
  - Ville de Caen
  - Pôle de compétitivité Aerospace Valley (AESE)
  - Région Aquitaine
  - DGA
  - …
- With Univesities
  - Université de Caen ; Laboratoires LITIS, XLIM, Valoria
  - ENAC
  - …

Laboratoire Bordelais de Recherche en Informatique

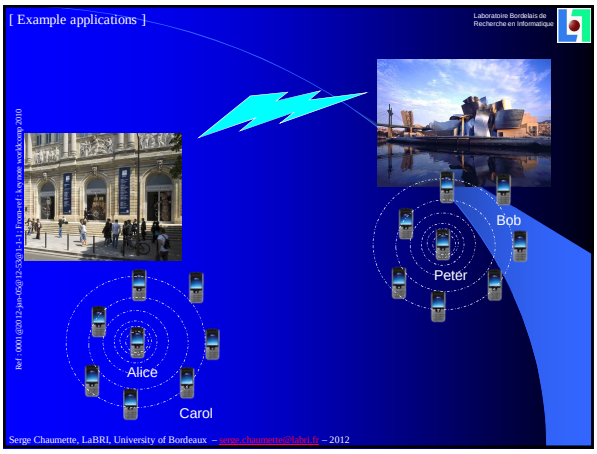
Strategic map sharing

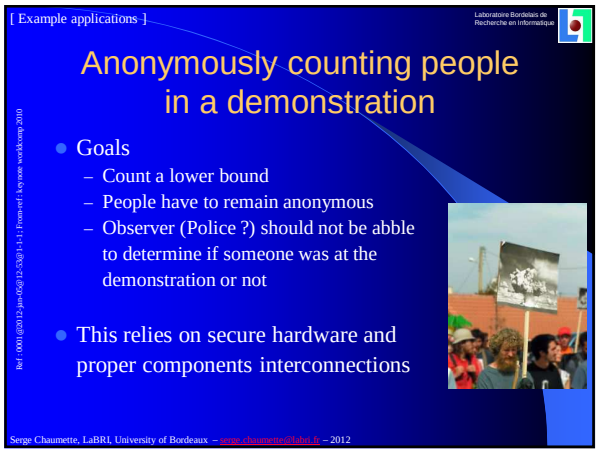
Map sharing (DGA)
[IEEE milcom]

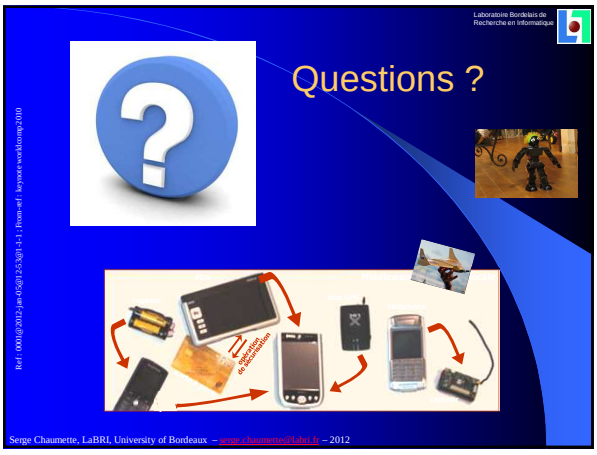
Laboratoire Bordelais de Recherche en Informatique

Museum Quest

- European project (ITEA2)
  - Smart Urban Spaces
  - http://www.smarturbanspaces.org/
- 25 partners, 4 countries
  - Gemalto, Thales, NXP, …
  - VTT, LaBRI, University of Caen
  - Valence, Bordeaux, Bilbao, …


[Example applications]
Laboratoire Bordelais de Recherche en Informatique
Bob
Peter
Alice
Carol
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


[Example applications]
Laboratoire Bordelais de Recherche en Informatique
Anonymously counting people in a demonstration
Goals
Count a lower bound
People have to remain anonymous
Observer (Police ?) should not be abble to determine if someone was at the demonstration or not
This relies on secure hardware and proper components interconnections
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012


Laboratoire Bordelais de Recherche en Informatique
Questions ?
Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2012