Une vision sociale des objets connectés et de leurs usages : aspects liés à leur sécurité

Jean-Paul Jamont
Maître de Conférences - HDR
Université Grenoble Alpes – IUT de Valence
Laboratoire LCIS – G.INP – UGA

jean-paul.jamont@lcis.grenoble-inp.fr

UNIVERSITÉ Grenoble Alpes

LCIS

Grenoble INP ESISAR

Contexte Applicatif

1. Les objets sont partout

- Objets logiques :
  - Web services,
  - Agents logiciels,
  - …
- Objets physiques :
  - Capteurs/Actionneurs,
  - RFID,
  - Withings,
  - Waterpebble,
  - Glowcaps,
  - Sniftag,
  - Botanicalls,
  - Rosetta Stone,
  - LIFX,
  - Sphero,
  - Nabaztag,
  - Ubooly,

Contexte Applicatif

1. Les objets sont partout

Deux grands types d'objets physiques

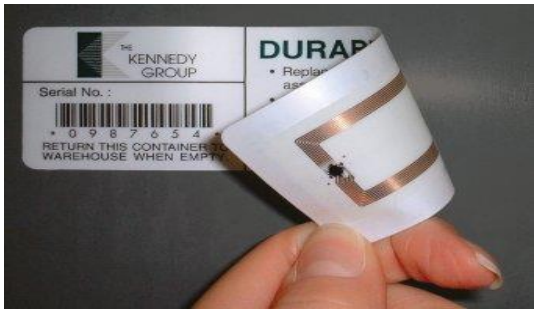
- Objets communicants et/ou intelligents

  A base de micro-contrôleur(s) /FPGA équipés d'interface(s) de communication

  ⇒ Modèle de COMPORTEMENT EMBARQUE sur l'objet

- Objets « chipless » tagués

  Objets sur lesquels on a apposé une étiquette RFID (ou autre)



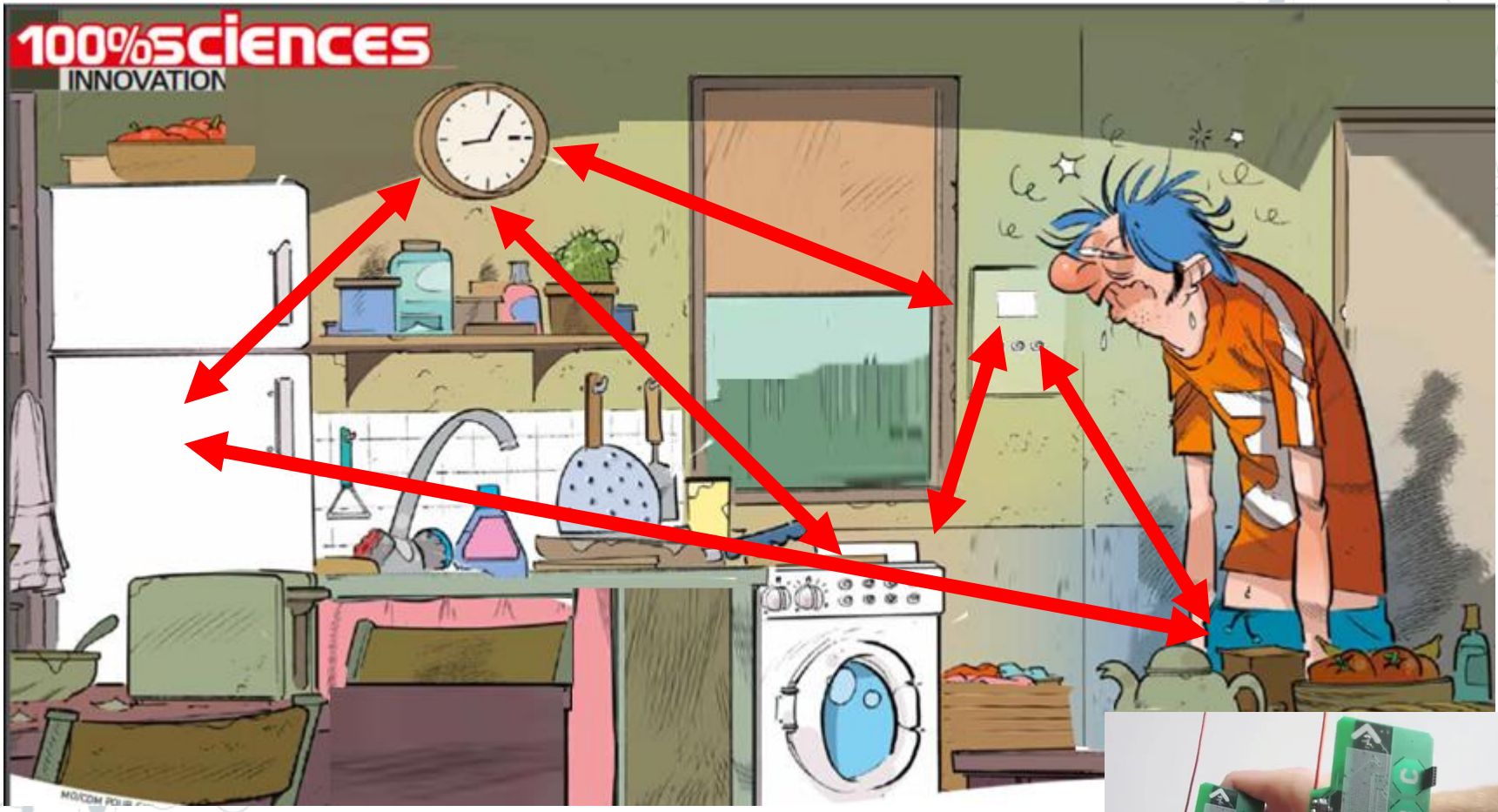
⇒ Modèle de COMPORTEMENT DEPORTE sur un serveur distant

Contexte Applicatif

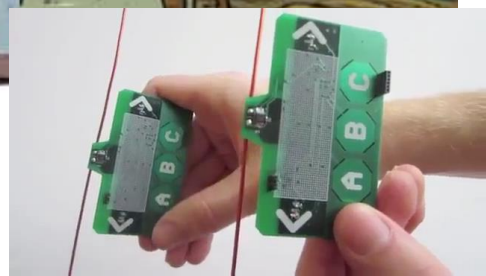
1. Les objets sont partout

Contexte Applicatif

2. Les objets parlent entre eux!

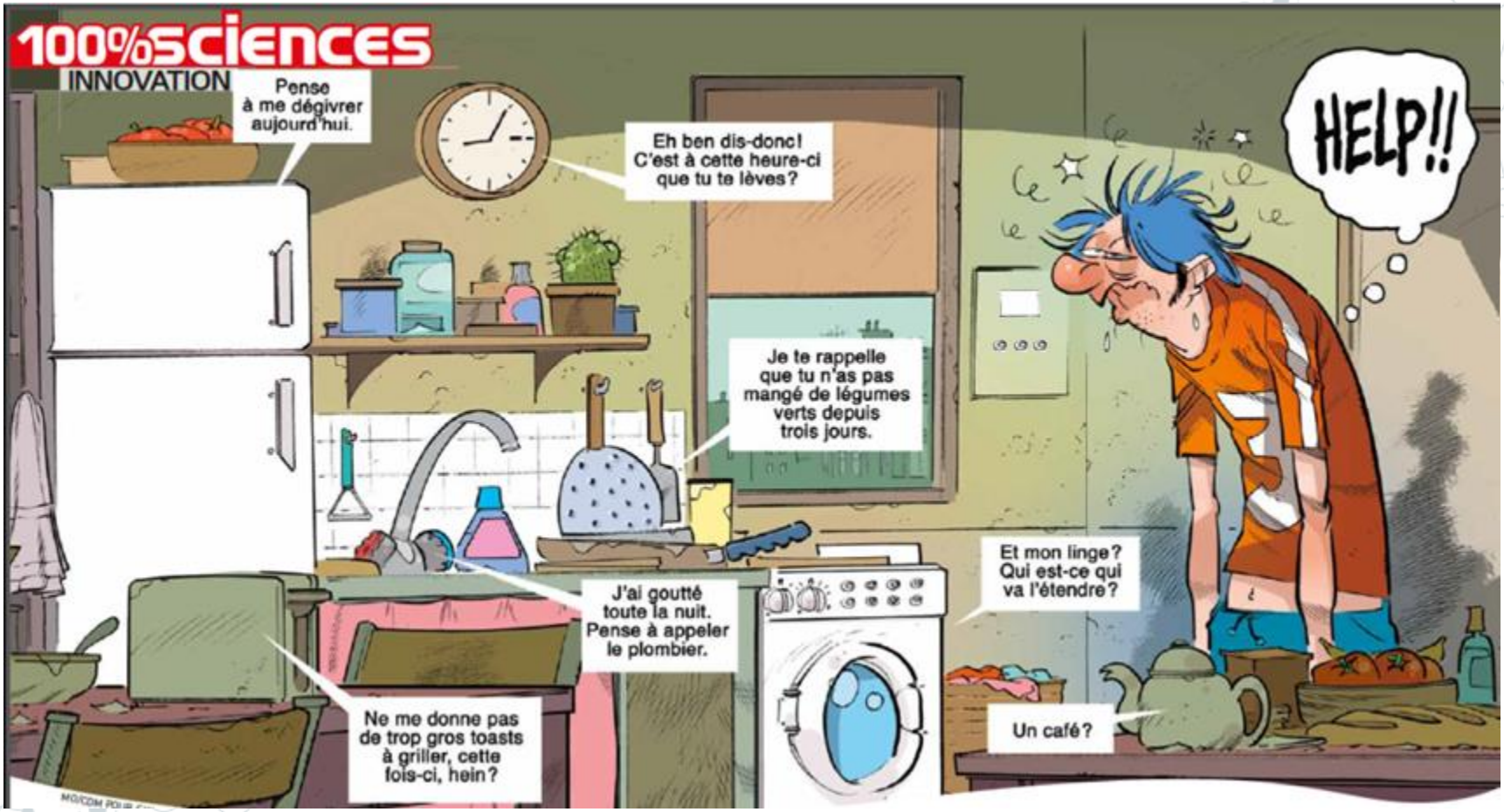


O. Lascar, Quand les objets nous parleront, SVJ-Janvier/2012. (librement modifiée)



Contexte Applicatif

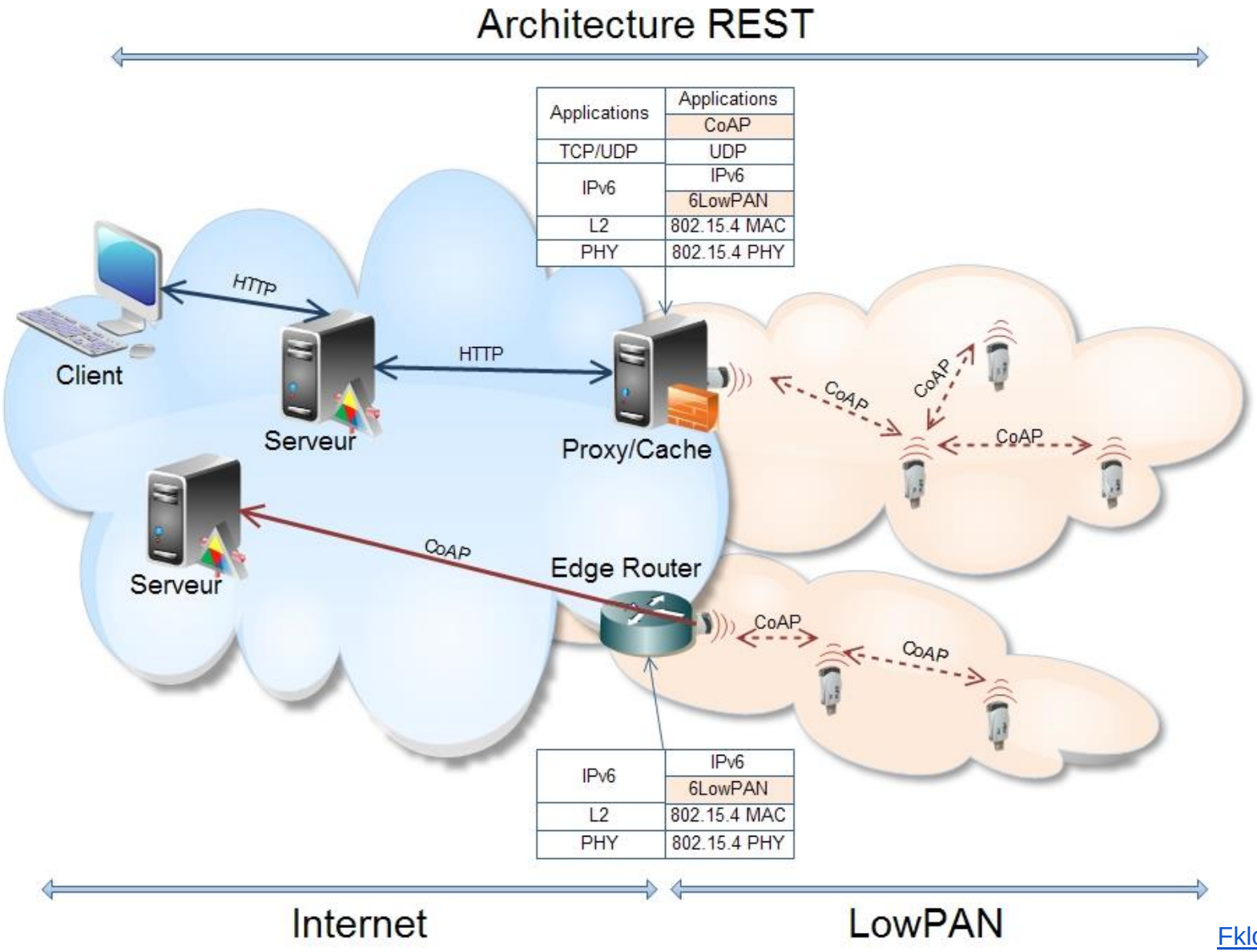
3. Ils parlent de nous!



O. Lascar, Quand les objets nous parleront, SVJ-Janvier/2012. (librement modifiée)

Contexte Applicatif

4. Ils ont accès à Internet



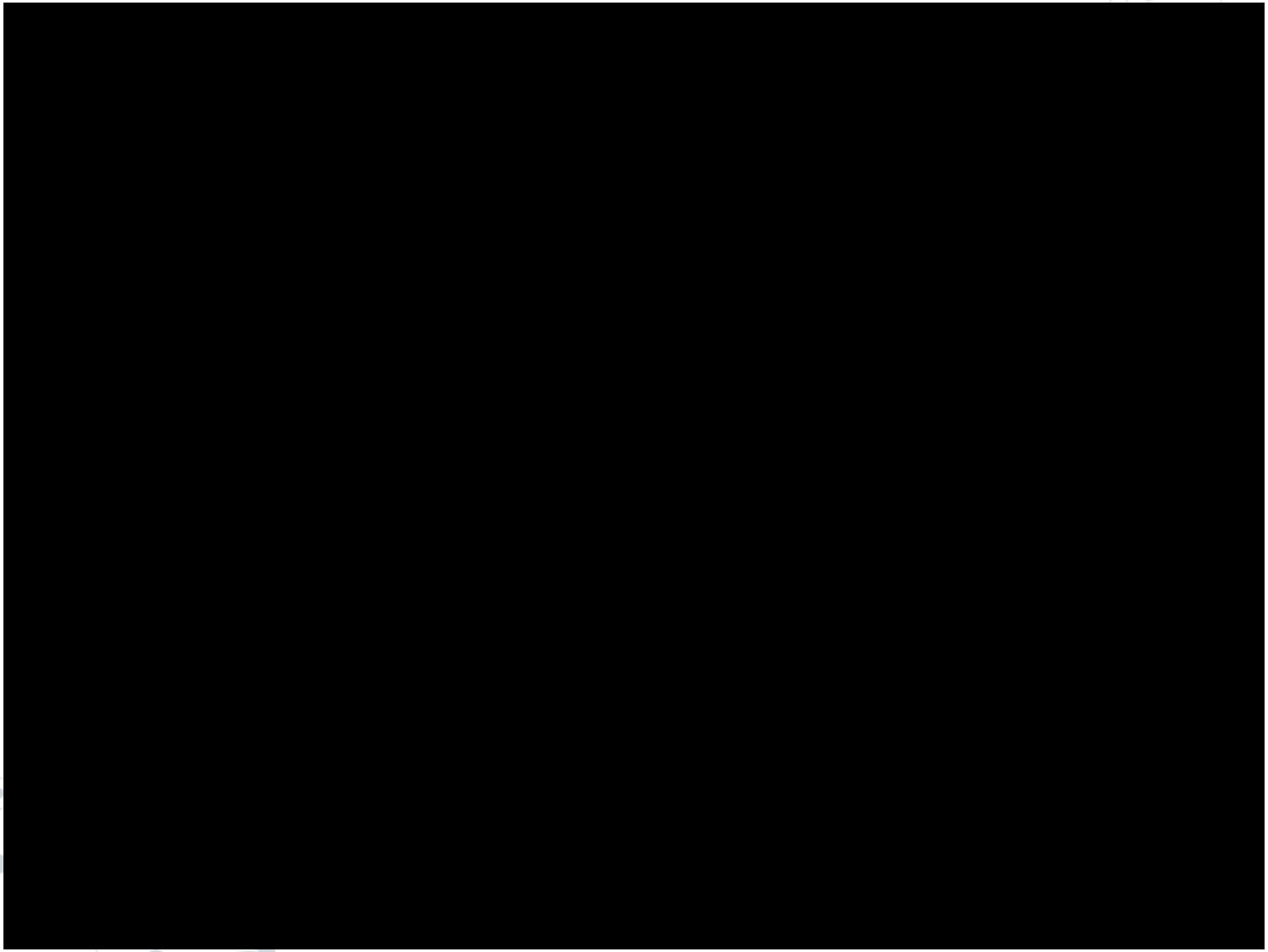
Fklopfenstein

Contexte Applicatif

Avènement du *Social Web of Things* (Ericsson)

Contexte Applicatif

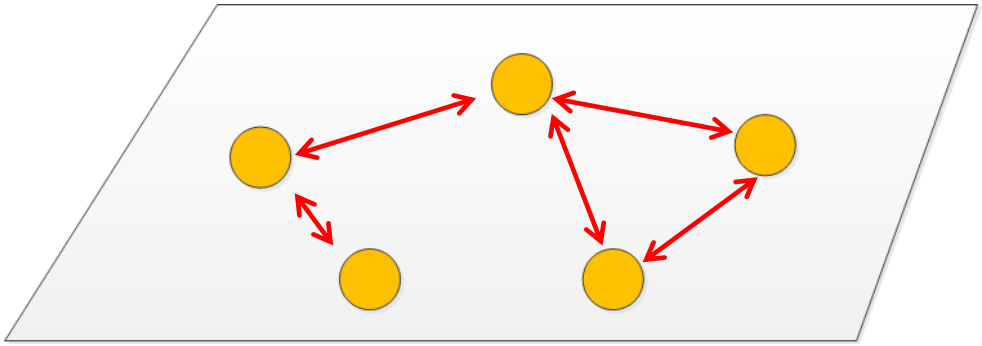
Large Scale Logistic Systems



Problématique

Des systèmes cyber-physiques

[Sztipanovits 2007, Lee 2008-13, NI 2014]

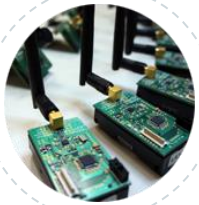


Problématique

Les propriétés des systèmes cyber-physiques

[Lee02, Elmenreich03, Henzinger06, Lee08, Pottie09, Lee13,Jamont16]

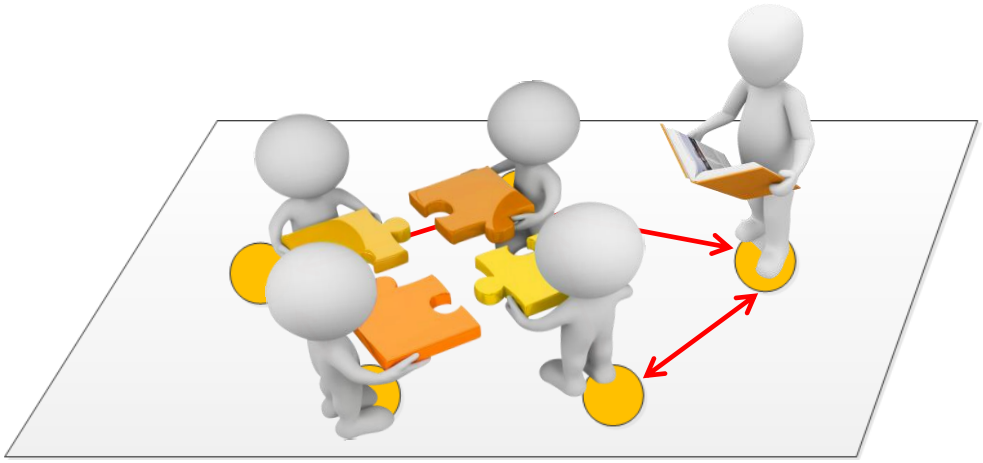
1. Réactivité,
2. Terminaison,
3. Ponctualité,
4. Autonomie d'énergie,
5. Gestion de la sécurité.



6. Complexité,
7. Concurrence,
8. Hétérogénéité multiple,
9. Intégration d'interfaces,
10. Reconfiguration et auto-organisation,
11. Mobilité,
12. Intégrité.

Problématique

Des collectifs cyber-physiques



Problématique

Les propriétés // la sécurité

- SÉCURITÉ DES BIENS ET DES PERSONNES
- DISPONIBILITÉ DE SES SERVICES…
- PROTECTION CONTRE LES ATTAQUES QUI VISENT À LE DÉTOURNER DE SA FONCTION ET/OU À EN PRENDRE LE CONTRÔLE.

- OUVERTURE
- LARGE ECHELLE
- HÉTÉROGÉNÉITÉ

- Sensibilité aux attaques malicieuses
- Frein à l'emploi de techniques classiques (PKI, TPM,credentials, …) de sécurité informatique

Problématique

Une ingénierie multi-agent des CCP

BESOINS APPLICATIFS

PROCESSUS GÉNIE LOGICIEL

SOLUTION
COLLECTIF CYBER-PHYSIQUE
SECURISE

Plan

1. Contexte applicatif et Problématique

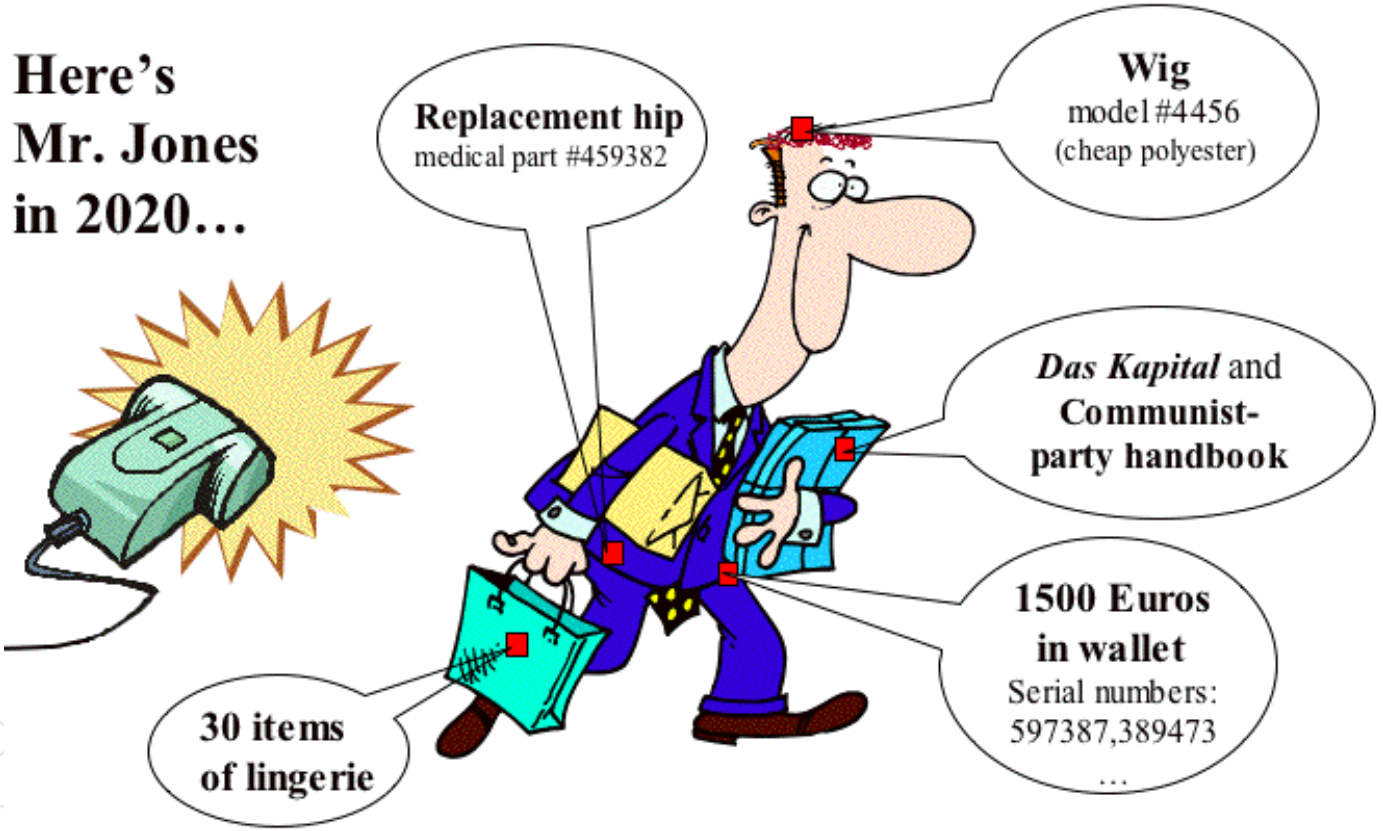
2. Privacité

3. Confiance et réputation

4. Une expérience dans le contexte des WSN

Privacité

DON'T THEY KEEP ANYTHING FOR THEMSELVES ??

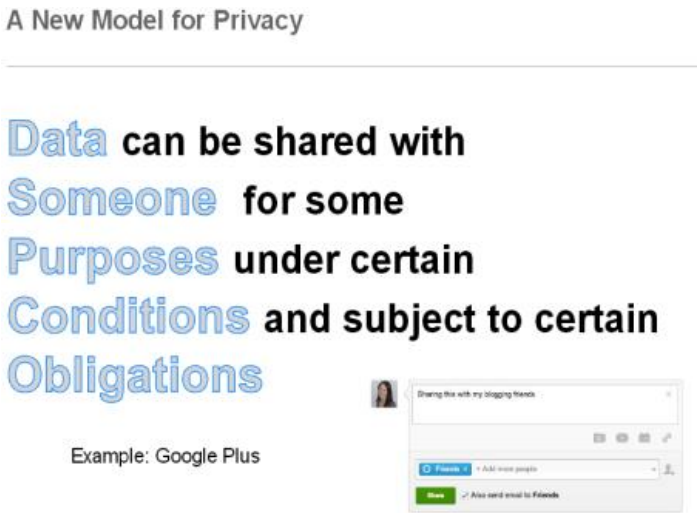


M. Jones en 2020 [Jue04]

Privacité

Six éléments constitutifs des politiques de protection des données personnelles:

1. Information de l'utilisateur,
2. son consentement,
3. son droit à modifier ou supprimer les données prélevées
4. la justification de la collecte de données personnelles,
5. la durée de conservation
6. les conditions de transmission de ces données



Privacité

- Objectifs:
  - Protection des données personnelles et de la vie privée
- Principes:
  - Communications IP & accès aux services anonymes
  - Gestion d'identités virtuelles multiples
  - Autorisations préservant la vie privée/Gestion des données personnelles
- Difficultés:
  - Diversité des informations
  - Nature relative du caractère sensible d'une information
  - Forte implication des utilisateurs

Plan

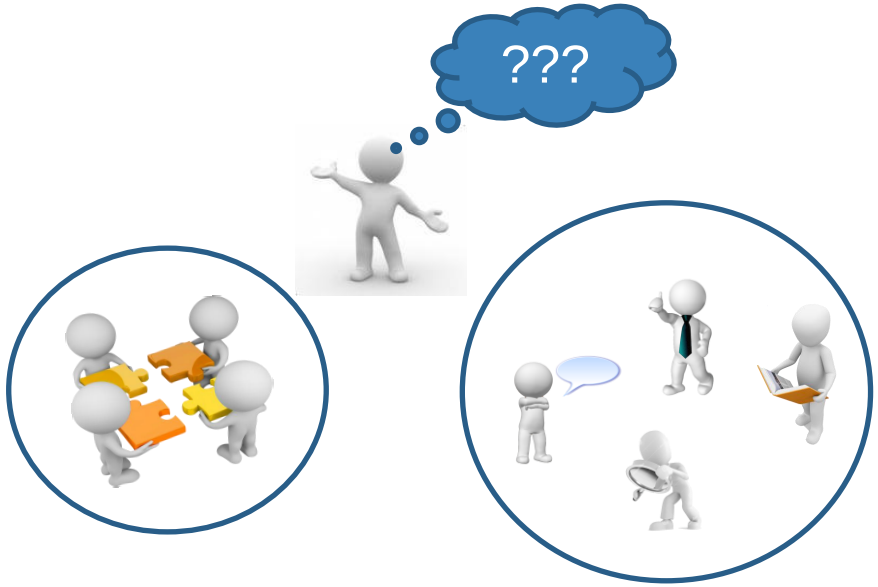
1. Contexte applicatif et Problématique
2. Privacité
3. **Confiance et réputation**
4. Une expérience dans le contexte des WSN

Confiance et Réputation

- Objectif :
  - Protéger l'utilisateur et les objets de mauvais comportements
- Principe :
  - Observer puis évaluer le bon comportement des entités
  - Sanctionner un mauvais comportement
  - Eviter les interactions avec les entités jugées indignes de confiance
    ⇒ Mécanisme de contrôle social
  - Implanter des mécanismes de l'oubli
- *Utiliser les valeurs de confiance calculées par les entités dignes de confiance (réputation)*
- Difficultés:
  - Intentionnalité
  - Multi-dimentionalité
  - Ouverture
  - Mobilité

Détection d'intention

- Objectif :
  - Comprendre la motivation d'une sollicitation
- Principe :
  - Observer les actions des entités
  - Comprendre les plans appliqués, l'organisation sociale du système
    ⇒ Détecter l'intention
- Difficultés:
  - Connaissances a priori
  - Ouverture
  - Mobilité



Plan

1. Contexte applicatif et Problématique
2. Privacité
3. Confiance et réputation
4. **Une expérience dans le contexte des WSN**

Une expérience dans le contexte des WSN

Trust management for WSN

Requirements for WSN:

- detection of deviant behaviors in node communications
- decentralization of trust management
- lightweight algorithms and mechanisms (CPU + mem restriction)

Many existing works in decentralized trust management

- in multi-agent systems [Sabater-Mir, Josang, Singh, Sen, …]
- in peer-to-peer systems [Despotovic, Vercouter, …]
- in ad hoc networks [Griffiths, …]
- in wireless sensor networks [Fernàndez-Gago,Yao, Ganeriwal…]

Provides means to implement a decentralized approach, but…

- they assume high communication and storage capacities

Une expérience dans le contexte des WSN

Trusted-MWAC

A specific trust model is necessary

- with simple trust calculation algorithms
- having low costs in communication/storage
- without authentication implying the absence of identity
- Trust must be estimated locally by each agent by supervising the messages sent in its neighborhood.
- Even if authentication is not possible, nodes have to use an id (real or fake) when sending a message.

$\Longrightarrow$ We propose to use trust in an `id` (rather than trust in an agent authentied with an `id`) in order to represent the way an id has been used in the past.

$\Longrightarrow$ The trust values in the neighboor `id` allow to know if we have a trusted neighboorhood or not.

Une expérience dans le contexte des WSN

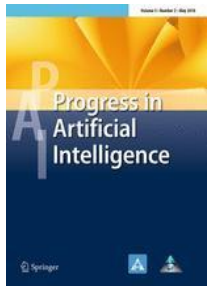
Trusted-MWAC

Main idea: trust in the neighbourhood:

- Node receives doubtful information from one of its neighbours.
- Trust in id *i* drops under threshold θ_1
- Neighbourhood of the node becomes distrusted
- Node switches to backup-mode, it :
  - doesn't take active role in the self-organization process
  - doesn't participate in routing functions anymore

When all the neighbours of the malicious node *i* begin to run in backup mode, the whole area containing *i* will become isolated.

⇒ This area of the network is in quarantine



Laurent Vercouter, Jean-Paul Jamont: Lightweight trusted routing for wireless sensor networks. Progress in AI : 193-202 (2012)

Une expérience dans le contexte des WSN

Trusted-MWAC

During the introduction step, agents exchange id informations

`<id,role,groups>`

Nodes may lie about:

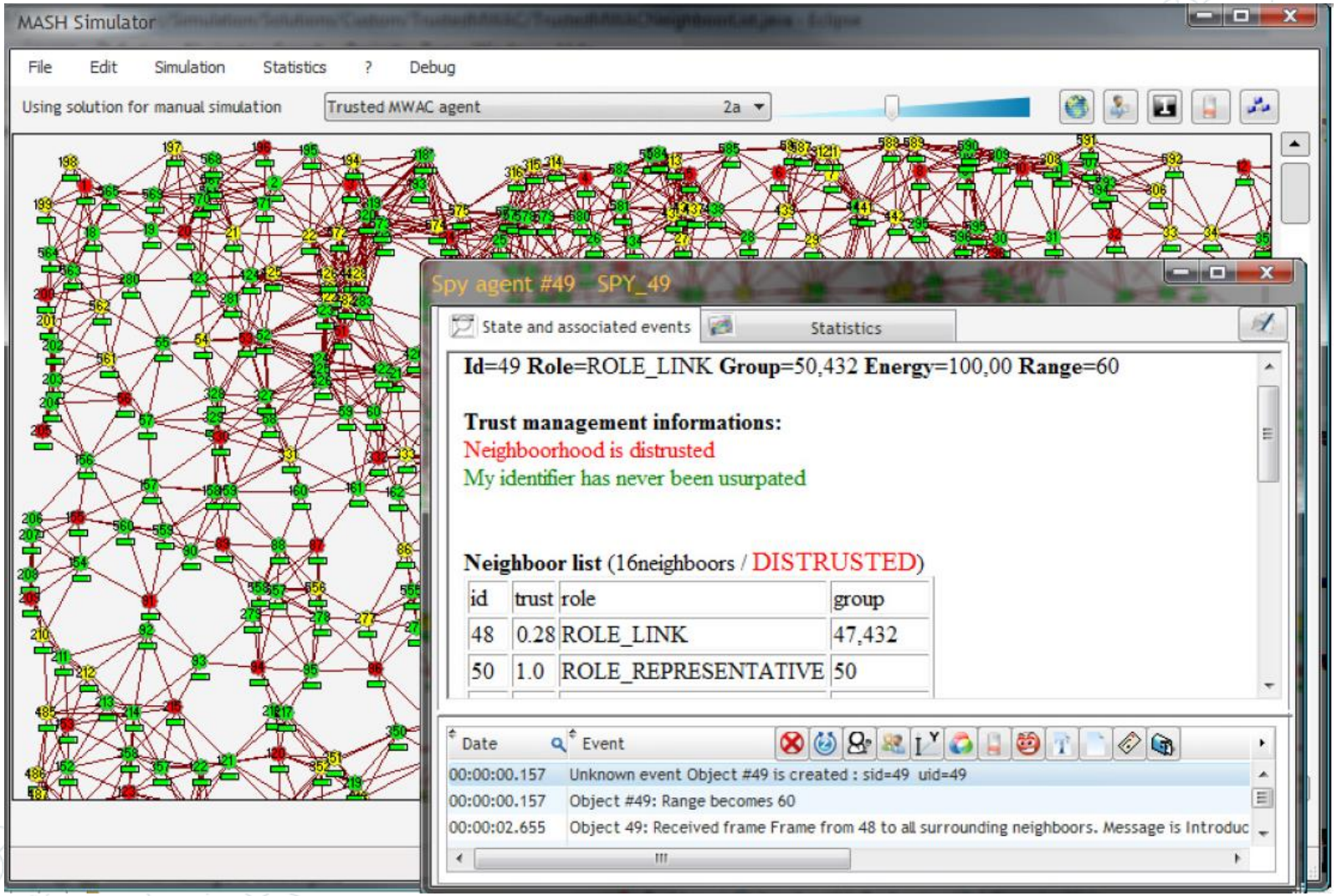
- Not include all the groups
- Claim they belong to a new group (for connection nodes)

- Claim they are a connection to a new group (the same as the previous)

- Steal the workstation's ID
- Steal a neighbour's ID

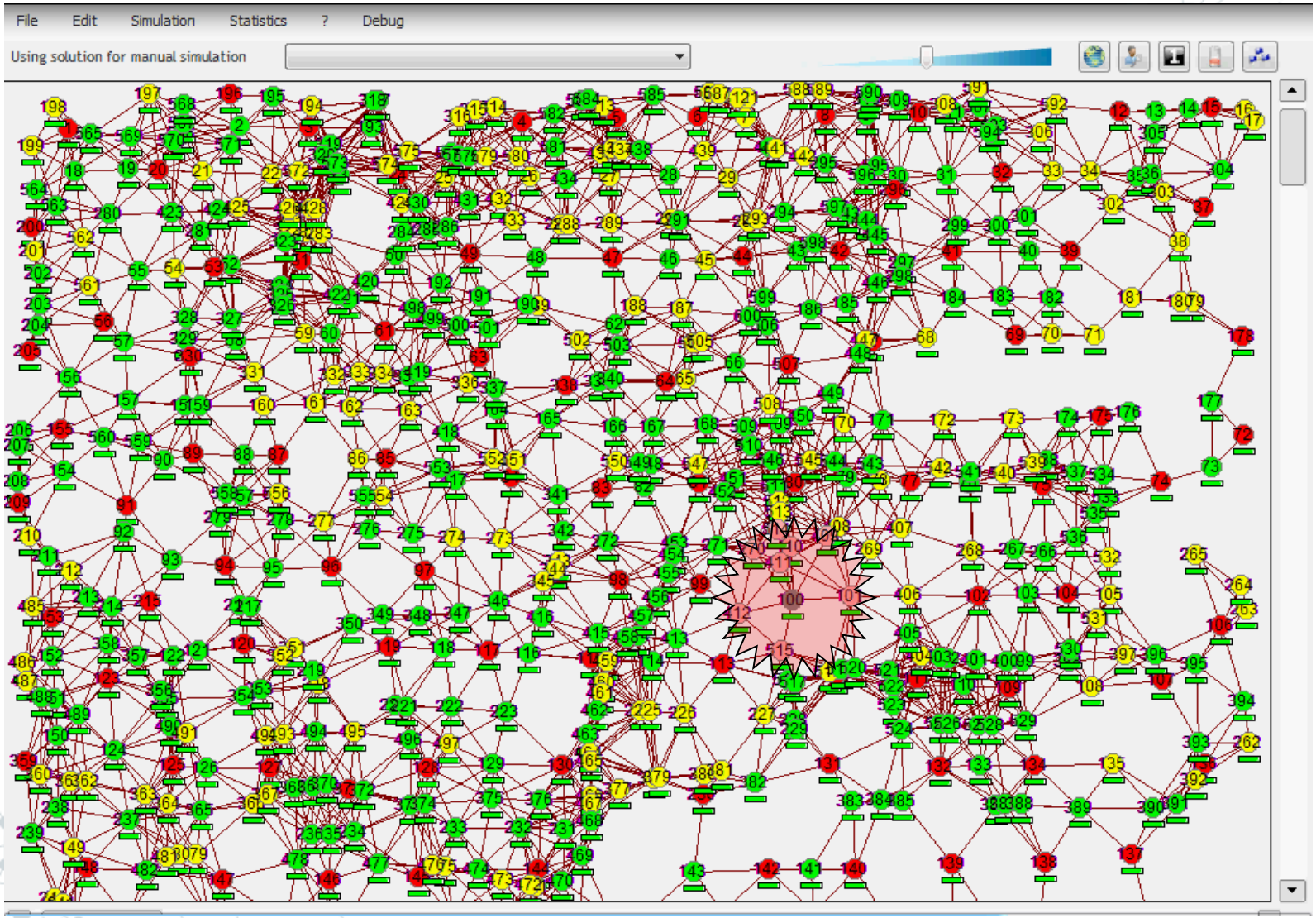
Une expérience dans le contexte des WSN

Smiulation step



Une expérience dans le contexte des WSN

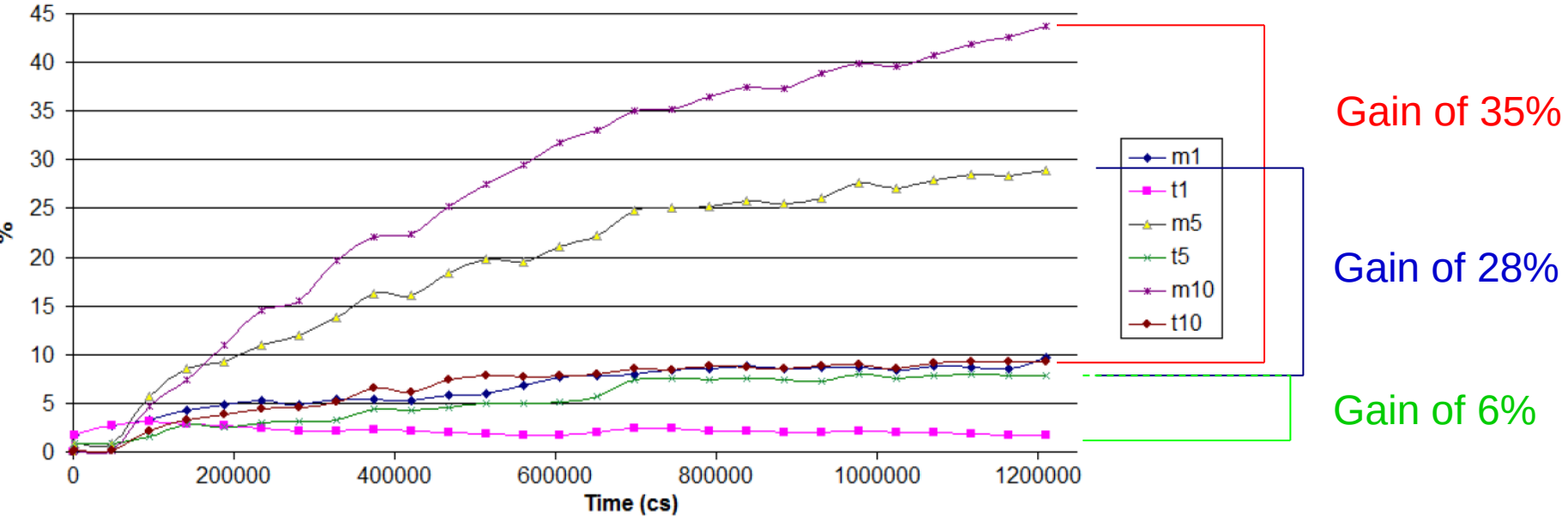
Création de zone de quarantaine



Une expérience dans le contexte des WSN

Résultats

* Additional occupation (java implementation):
  - Size of the code : increased by 10%
  - Data memory required for neighboorhood management: increased by 20%
* Result for a specific scenario (600 sensor agents, 1/5/10 liars):



Pourcentage of missing measures

Conclusion

Une approche sociale des objets connectés

Dans le contexte des systèmes ouverts à large échelle à intelligence décentralisée:

- Criticité des modèles de gestion de la confiance, de la réputation, de la privacité
- Domaines de recherche très actifs

Intérêt pour MACY-COSY@LCIS:

- Une brique importante des systèmes embarqués à intelligence collective

Projets en cours:

- Cyber résilience (Thalès)
- ANR ASAWoO (Génération Robot, LIRIS, IRISA)
- Projet coopératif LCIS & LITIS

Merci de votre attention