



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`

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

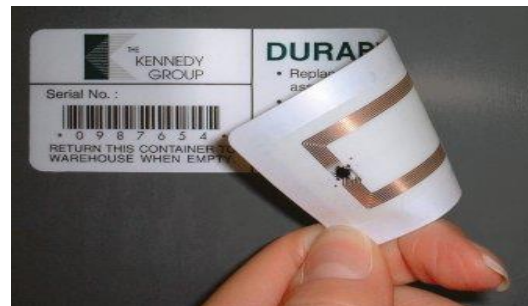
- Objets communicants et/ou intelligents

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

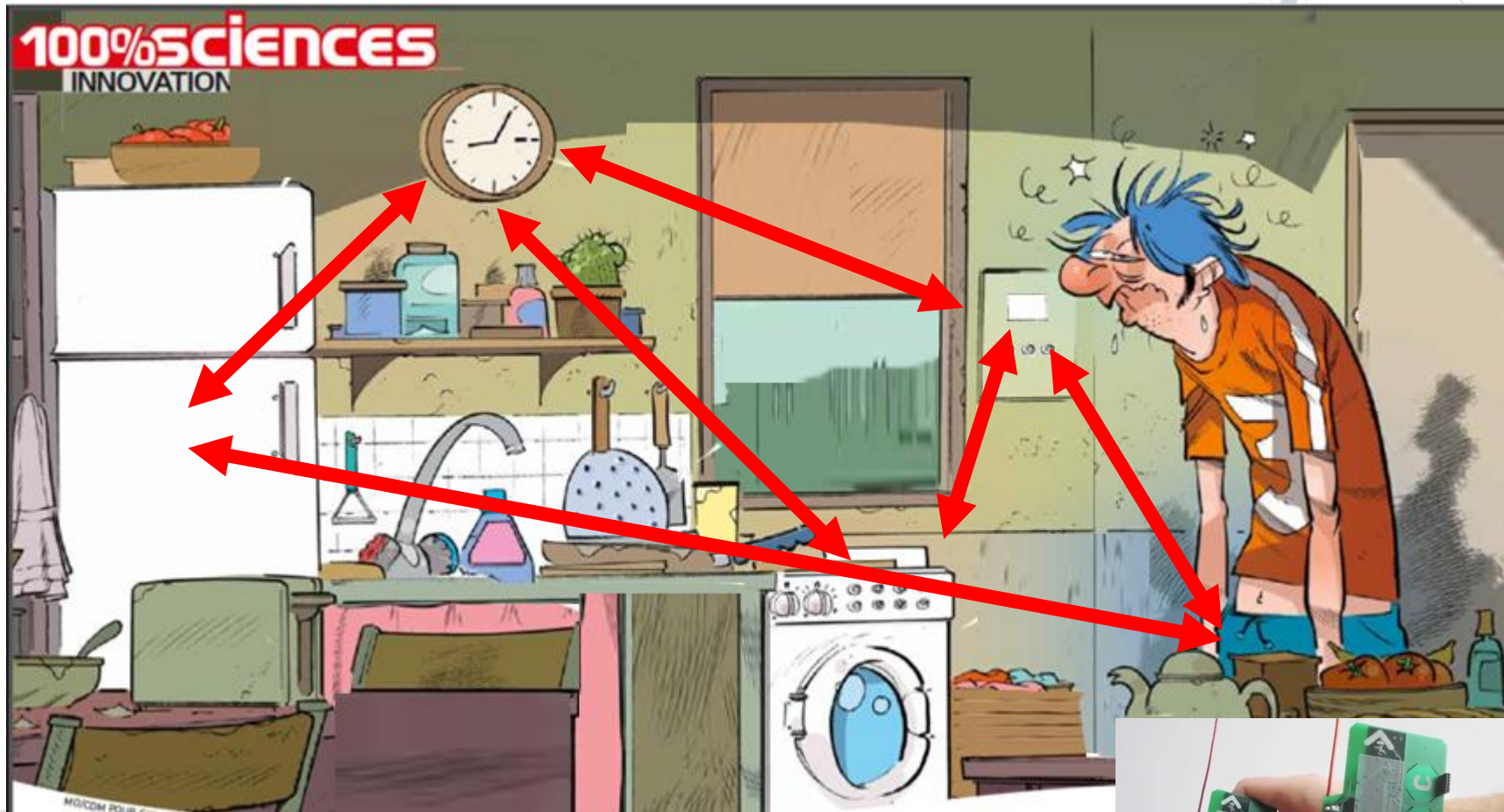
Contexte Applicatif

1. Les objets sont partout

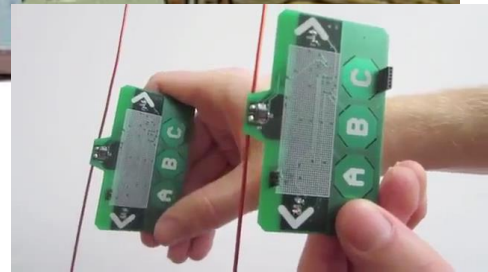


Contexte Applicatif

2. Les objets parlent entre eux!

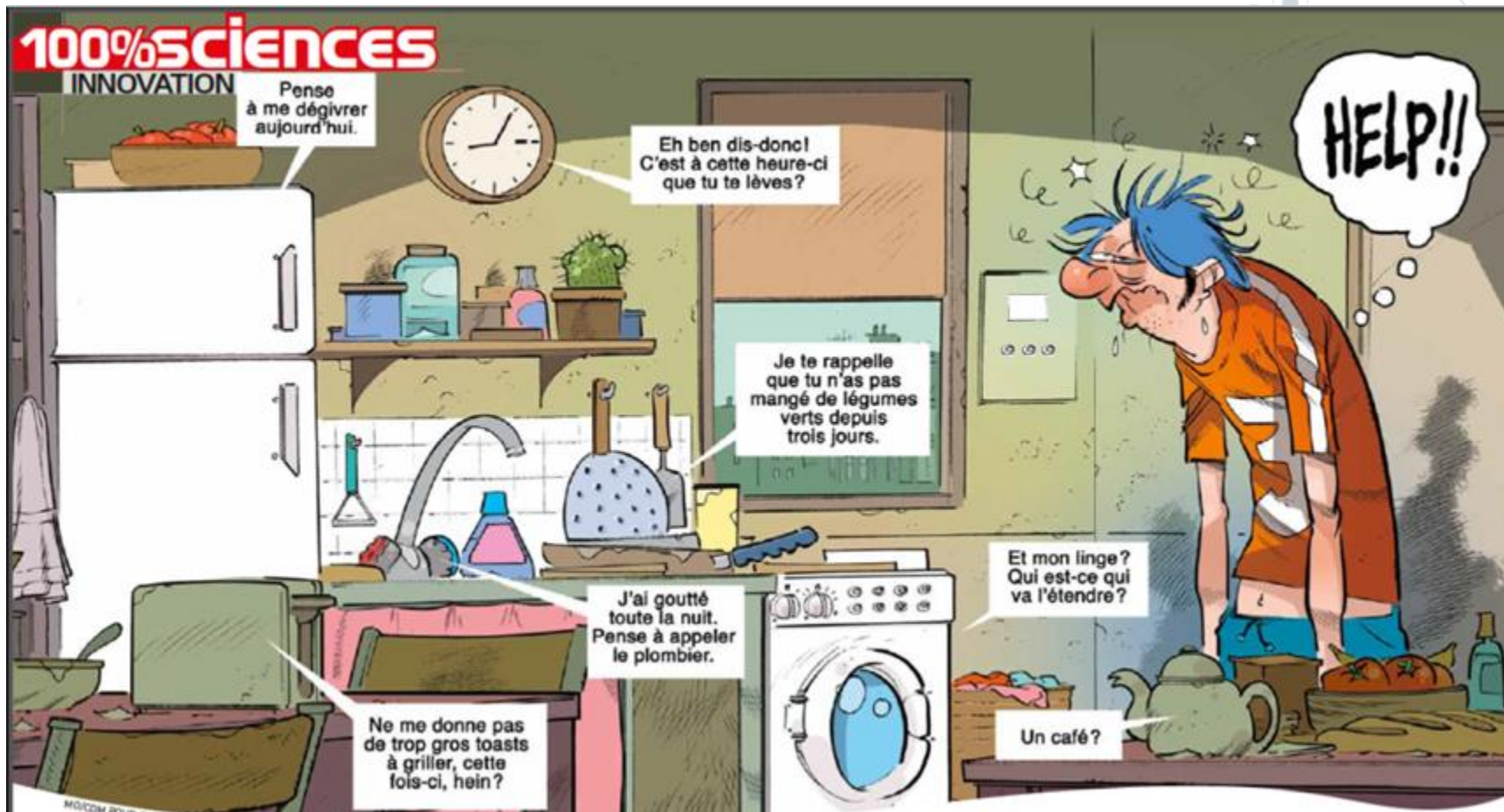


O. Lascar, Quand les objets nous parleront, SVJ-Janvier/2012. (librement modifiée)



Contexte Applicatif

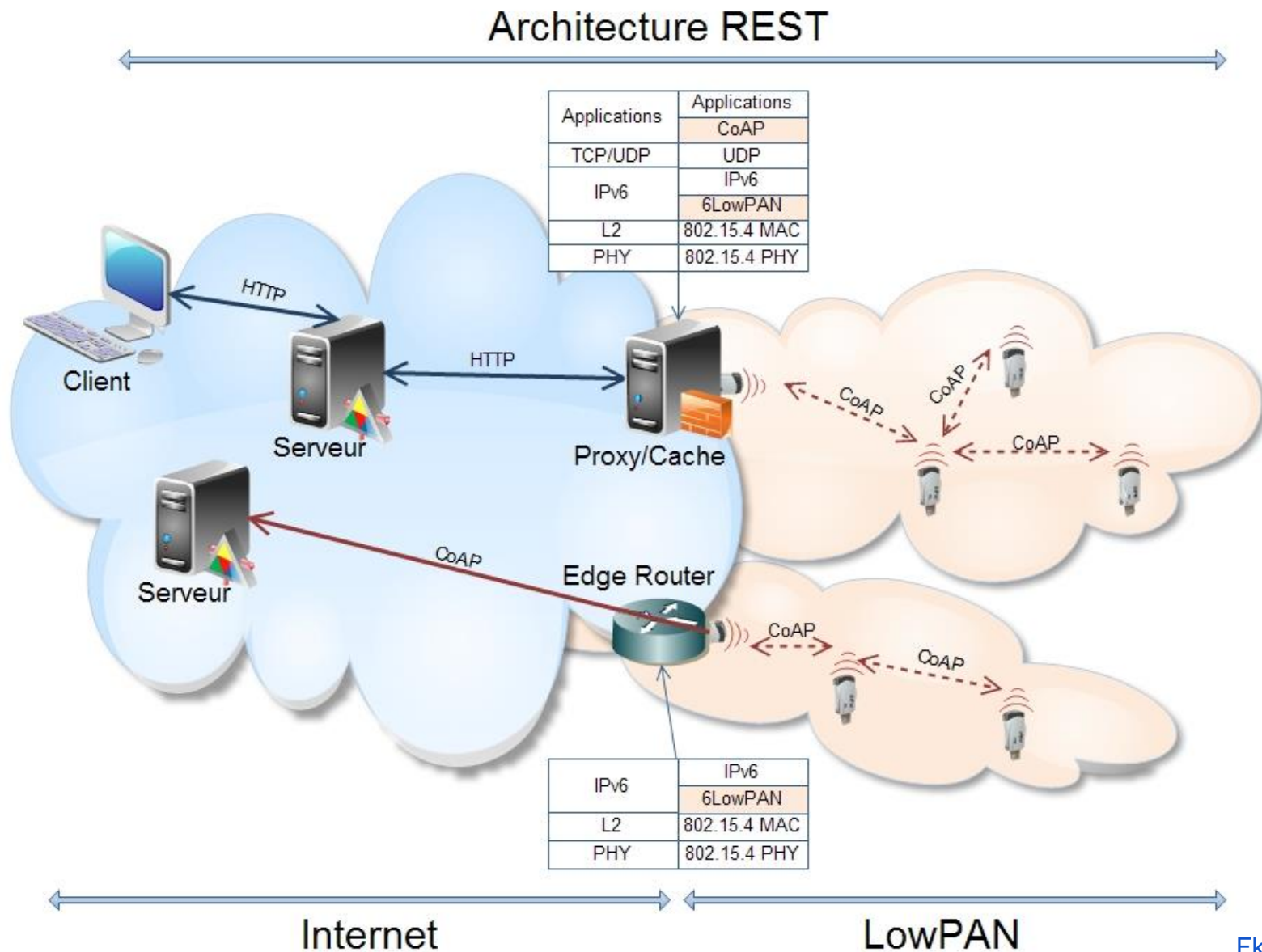
3. Ils parlent de nous!



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

Contexte Applicatif

4. Ils ont accès à Internet



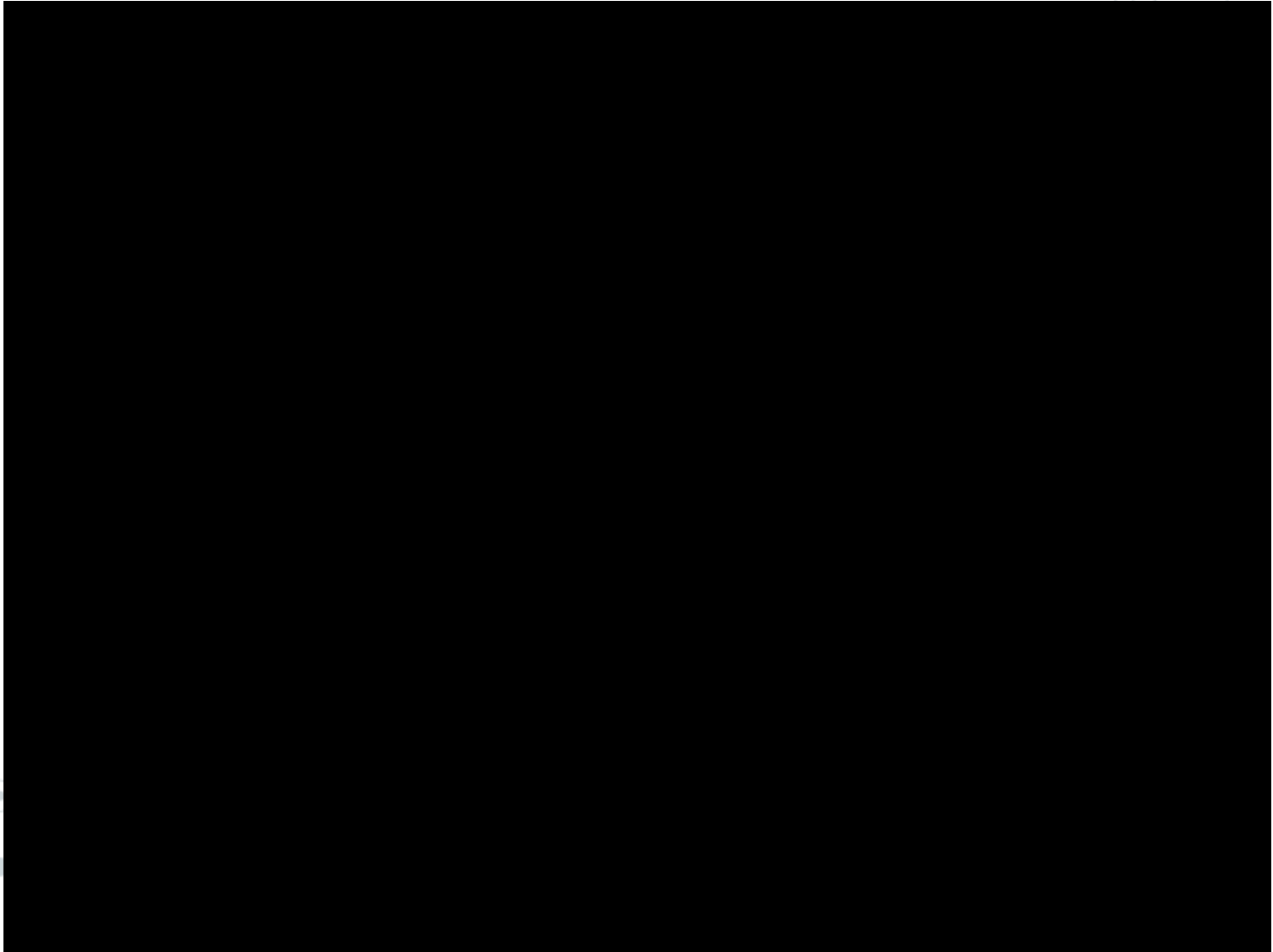
Contexte Applicatif

Avènement du *Social Web of Things* (Ericsson)



Contexte Applicatif

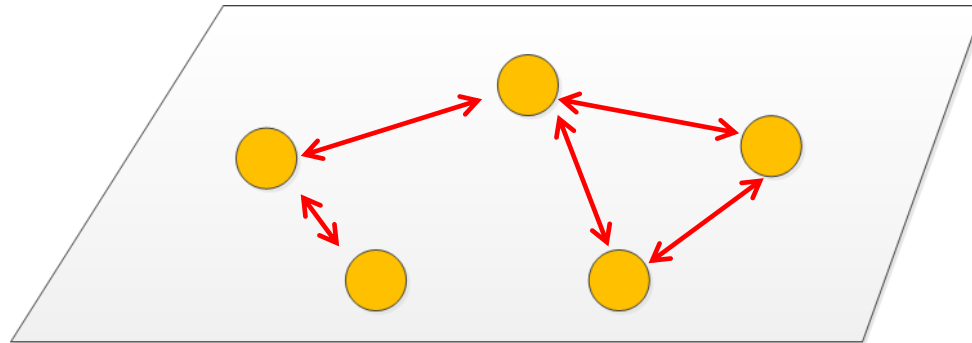
Large Scale Logistic Systems



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]



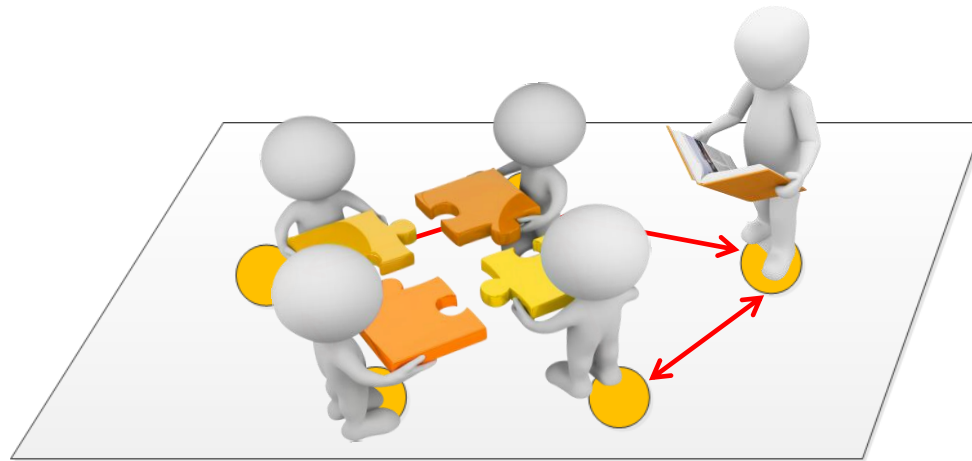
1. RÉACTIVITÉ,
2. TERMINAISON,
3. PONCTUALITÉ,
4. AUTONOMIE D'ÉNERGIE,
5. GESTION DE LA SÉCURITÉ.



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 ÉCHELLE
- ◎ HÉTÉROGÉNÉITÉ

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

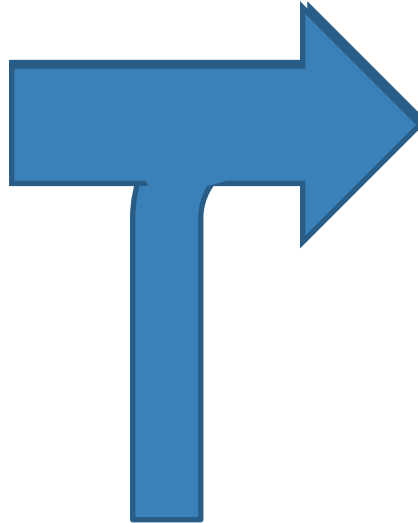
Problématique

Une ingénierie multi-agent des CCP

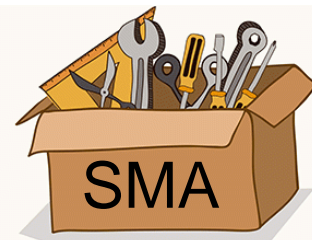


BESOINS APPLICATIFS

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



Privac  



DON'T THEY KEEP ANYTHING
FOR THEMSELVES ??

**Here's
Mr. Jones
in 2020...**

Replacement hip
medical part #459382

Wig
model #4456
(cheap polyester)

***Das Kapital* and
Communist-
party handbook**

**1500 Euros
in wallet**
Serial numbers:
597387,389473
...

**30 items
of lingerie**

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

A New Model for Privacy


Data can be shared with
Someone for some
Purposes under certain
Conditions and subject to certain
Obligations

Example: Google Plus



Privacité

A decorative network diagram in the top right corner, consisting of a series of interconnected nodes (circles) and lines, representing a complex system or data flow.

- 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
- 
- A decorative network diagram in the bottom left corner, consisting of a series of interconnected nodes (circles) and lines, representing a complex system or data flow.

Plan

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



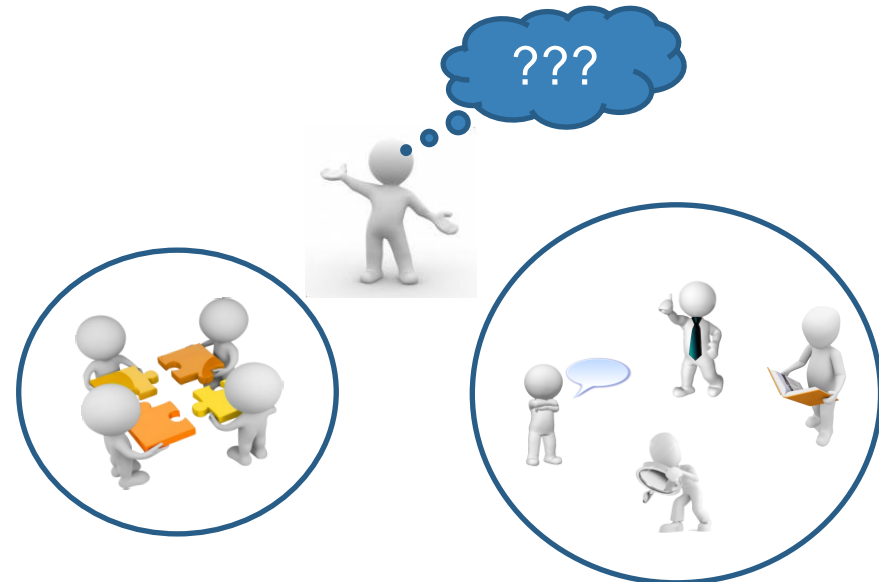
Confiance et Réputation



- 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-dimentionnalité**
 - **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 [Fernández-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.

⇒ We propose to **use trust in an id** (rather than trust in an agent authenticated with an id) in order to represent the way an id has been used in the past.

⇒ The trust values in the neighbor id allow to know if we have a **trusted neighborhood 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**

25 *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

Simulation step

The screenshot displays the MASH Simulator interface. The main window shows a network of nodes (represented by small icons) connected by red lines, indicating communication links. The nodes are color-coded, with green and red being prominent. A menu bar at the top includes File, Edit, Simulation, Statistics, ?, and Debug. Below the menu, there's a status bar indicating 'Using solution for manual simulation' and a dropdown menu set to 'Trusted MWAC agent'.

Overlaid on the main window is a smaller window titled 'Spy agent #49 - SPY_49'. This window has two tabs: 'State and associated events' and 'Statistics'. The 'State and associated events' tab is active, showing the following information:

Id=49 Role=ROLE_LINK Group=50,432 Energy=100,00 Range=60

Trust management informations:
Neighborhood is distrusted
My identifier has never been usurpated

Neighbor list (16neighbors / DISTRUSTED)

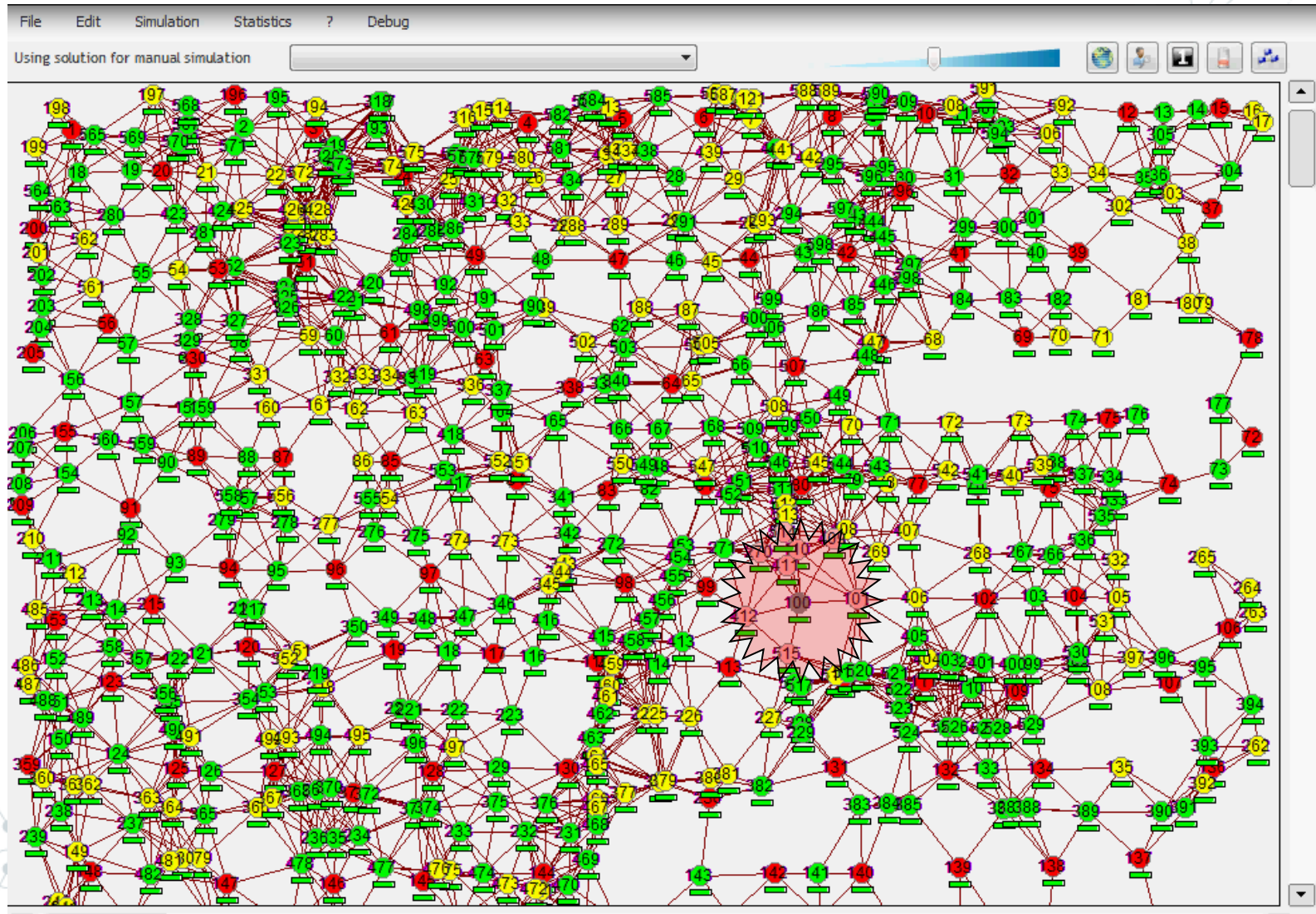
id	trust	role	group
48	0.28	ROLE_LINK	47,432
50	1.0	ROLE_REPRESENTATIVE	50

At the bottom of the 'Spy agent' window is an event log with columns for 'Date' and 'Event'. The log shows the following events:

- 00:00:00.157 Unknown event Object #49 is created : sid=49 uid=49
- 00:00:00.157 Object #49: Range becomes 60
- 00:00:02.655 Object 49: Received frame Frame from 48 to all surrounding neighbors. Message is Introduc

Une expérience dans le contexte des WSN

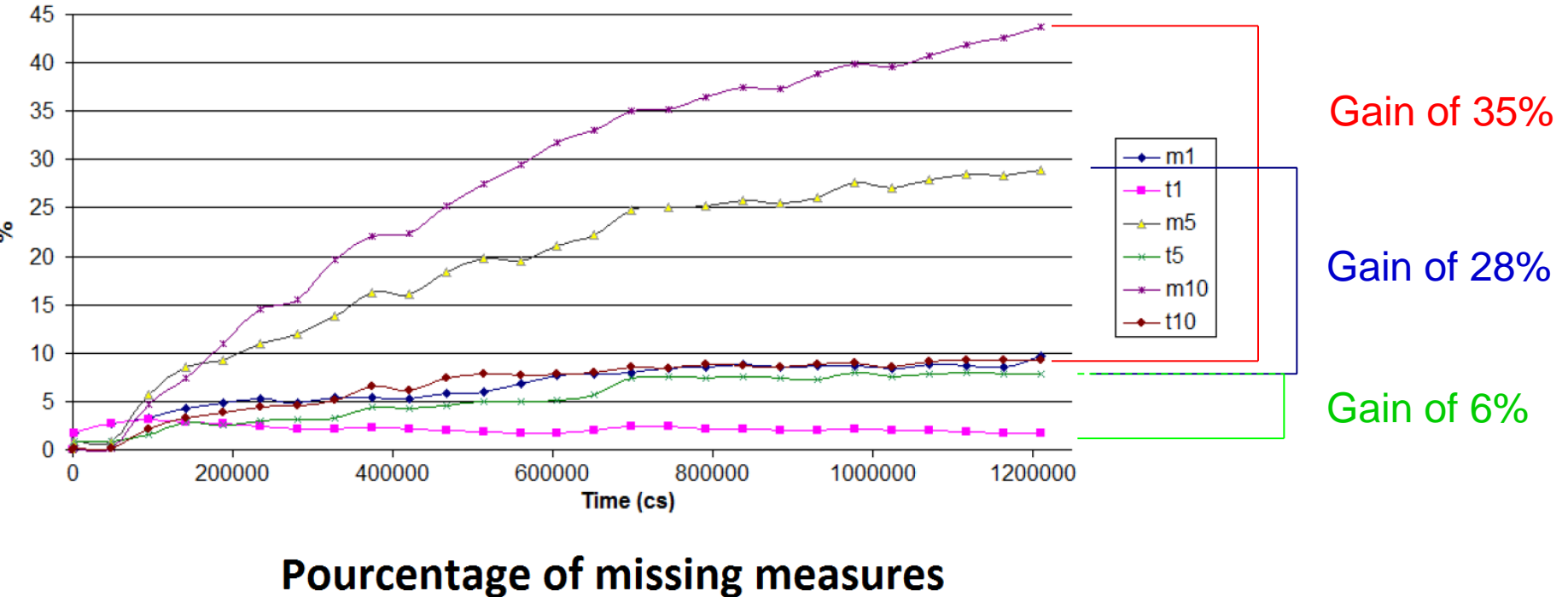
Création de zone de quarantaine



Une expérience dans le contexte des WSN

Résultats

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



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

