INSTITUT
Mines-Télécom

Internet des objets : Quels sont les freins à la protection des données personnelles ?

Séminaire Confiance numérique

Maryline LAURENT,
Institut Mines-Télécom/Télécom SudParis
Resp. Equipe R3S, CNRS SAMOVAR UMR5157
Cofondatrice de la chaire Valeurs et politiques des informations personnelles

MINES Albi-Carmaux · MINES Alès · MINES Douai · MINES Nantes · MINES ParisTech · Ecole Nationale Supérieure des Mines Saint-Etienne · TELECOM Bretagne · TELECOM Management · TELECOM ParisTech · TELECOM SudParis · EURECOM · TELECOM Lille · MINESnancy

MARCHÉ DU MOBILE : LES CHIFFRES

Smartwatch : 5 M vendues en 2014

Google play

25,5 MdS de $ de CA en 2015

320 M de personnes écoutent de la musique en streaming

Objets connectés

33 Mds d'objets connectés en 2020
et 50% des connexions INTERNET
Un marché de **320 milliards $** d'ici à 2022

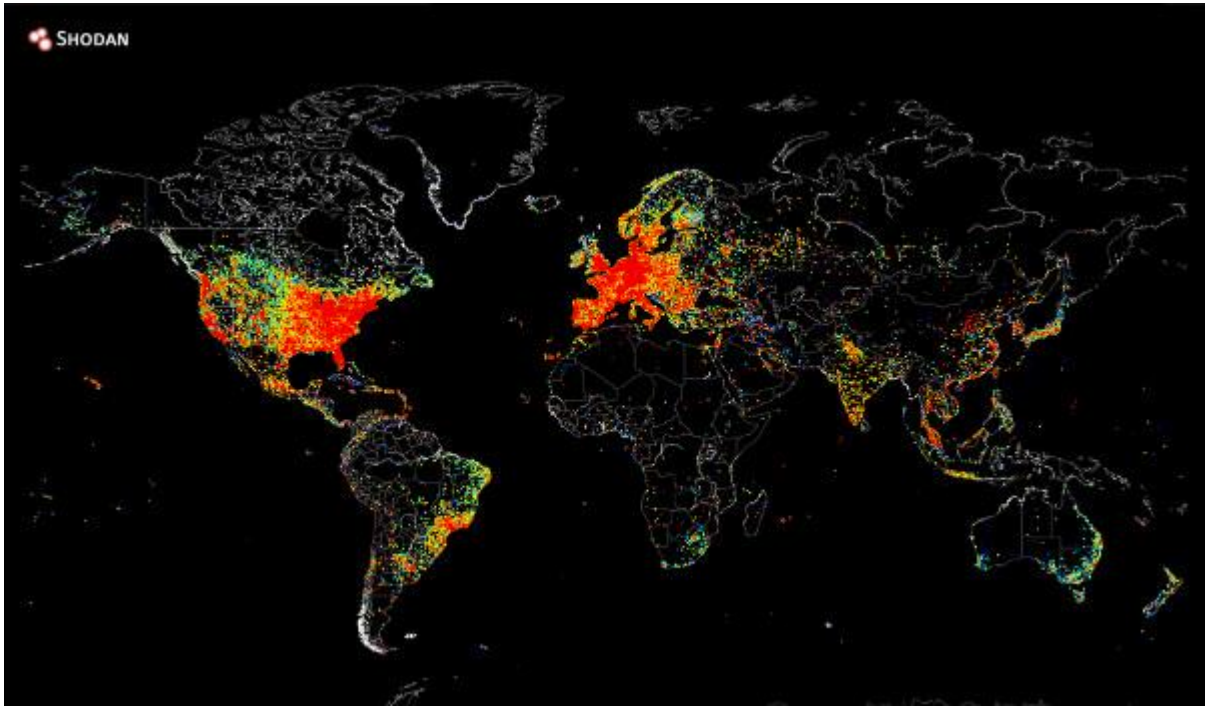
4G/LTE : couverture de 42% de la population en 2015
4G : 58% du trafic mobile en 2015
4G : Apple 1er vendeur en 2014 (34% de PDM)

<Balises Infos>

Fabrice@balises.info

Source : strategyanalytics.com

Grand succès des objets connectés aux USA et Europe



(Août 2014 - Source Shodan - moteur de recherche des objets connectés controversé) :
Points rouges : densité la plus élevée en appareils pouvant se connecter à Internet

Agenda

- **Définition de l'IoT**
- **Bref détour du côté de la législation**
- **Problématique technique propre à l'Internet des objets**
- **Solutions techniques**

Définition de l'Internet des objets (définition de IDC étendue)

- Réseau de réseaux d'objets
- Communications sans interaction humaine
- Connectivité IP
- Objets de plus en plus intelligents
- Objets capables de collecter des données, de prendre des décisions localement ou collectivement
- Externalisation possible des données et des décisions dans un cloud
- Objets physiquement vulnérables
- Mises à jour logiciel difficiles

Bref détour du côté de la législation Européenne avec la Directive de 1995

- **Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE n° L 281 du 23 novembre 1995**
- **Une donnée à caractère personnelle :** toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement
- **Directive de 1995 émet les principes suivants (non exhaustif) :**
  - Qualité des données personnelles : « finalités déterminées, explicites et légitimes »; « données adéquates pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées »;
  - Légitimation des traitements de données (consentement entre autres)
  - Sécurité et confidentialité des traitements

La législation Européenne : Où en sommes-nous ?

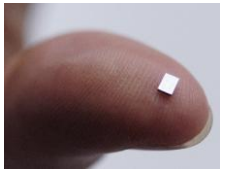
- **L'Union Européenne tarde à adopter le règlement GDP (General Data Privacy) dont le premier draft a été émis en 2012**

- **Le G29 a émis un avis en 2014**
  - Groupe G29 créé suite à l'article 29 de la Directive 95/46/CE
  - Groupe Article 29, *Opinion 8/2014 on the on Recent Developments on the Internet of Things, a*dopted on 16 September 2014, WP223
  - Données même pseudonymisées ou anonymisées sont des données personnelles dans l'IoT
  - Loi UE s'applique à tout responsable de traitement des données personnelles (situé UE, hors UE), dès lors que l'équipement IoT émetteur (réveil connecté, smartphone…) se trouve dans un pays membre
  - Principes d'importance : Consentement de l'utilisateur ; finalités déterminées, explicites et légitimes ; minimisation des données ; délai de conservation
  - Distingue plusieurs rôles des resp. de traitement : fabricants d'objets/OS, développeurs d'applications, plate-formes sociales

Problématique technique propre à l'Internet des objets

- Diversité des technologies
- Diversité des usages
- Diversité des architectures
- Difficulté de traiter la « protection des données personnelles »

Diversité des technologies



(source : numerama.com)

- **Composants : RFID, capteurs, puces (NFC, SIM), smartphones**
- **Communications à portée plus ou moins grande :**
  - ISO 18000-6C, ISO/CEI 14443 A/B, Zigbee, NFC (ISO 15693), 3G/4G, Bluetooth…
- **Capacités très hétérogènes :**
  - RFID : classiquement 80 kbps, qq centaines de bits mémoire, 7.500 à 15.000 portes logiques
  - Capteur : pour le Wismote jusque 250kbps en zigbee, 16 Ko RAM, 128 Ko ROM, µproc. 16bits
  - Smartphone : classiquement une centaine de Mbps (4G), 1Go RAM, 16 Go de ROM, processeur de 64 bits

Diversité des usages

- **Quantified self**
  - Activité Pop, la montre qui mesure toutes vos activités
  - Apple Watch
  - …
- **Domotique**
  - Smarter, la machine à café connectée
  - Wake, un réveil lumineux et sonore intelligent
  - SmartTV de Samsung (avec contrôle vocal ou reconnaissance faciale)
  - …
- **Santé**
  - Quell, un appareil de santé connecté pour soulager les douleurs
  - Oral-B SmartSeries, la brosse à dents connectée
  - …
- **Voiture connectée**
  - Auto-radio connecté (Pioneer + Google) grâce à Android Auto (disponible sur Google Play Store)
  - Application Blue Link (pour Hyundai récente) pour Android Wear et Apple Watch (démarrer/couper le moteur, verrouiller ou déverrouiller les portes, position GPS du véhicule, appel de secours)





Diversité des architectures

- **Centrée Smartphone**
  - Applications sur smartphone
  - Stockage/traitement des données localement ou dans le cloud
  - Hérite des vulnérabilités des smartphones (malwares, …)
- **Stockage / traitement des données dans le cloud**
  - Meilleure ubiquité
  - Hérite des vulnérabilité du cloud, nécessite de connecter un objet sur Internet
  - Ex : Amazon Echo, assistant personnel à commande vocal
- **En interaction avec d'autres objets**

Amazon Echo, assistant personnel à commande vocal

Réflexion sur la difficulté à protéger les données personnelles

- **Protection des données personnelles vs sécurité**
  - Traditionnellement dans la sécurité SSI :
    - Objectif : protéger une cible de sécurité (ITSEC)

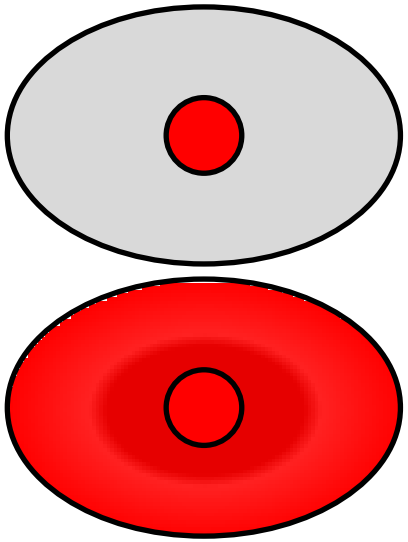
    Ex : serveur, réseau, données sensibles

    Périmètre défini avec précision
  - Protection des données personnelles dans un SI:
    - Objectif : éviter la fuite d'information non maitrisée

    En plus des données centrales à protéger, il faut protéger toutes les données périphériques

    Difficulté = le complémentaire du problème SSI

    Périmètre diffus, protection à assurer sans limite (cross layer, croisement de données)



Solutions techniques

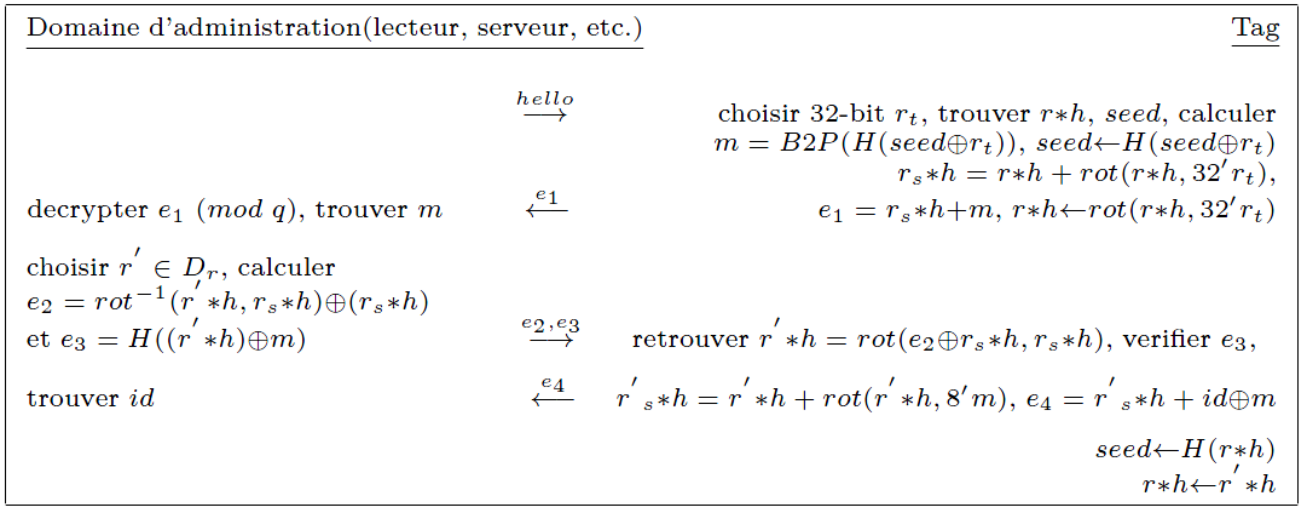
- **Standardisation par technologie, parfois par usage**
  - Répondant à un cahier des charges (p.ex. exigences de sécurité) plus ou moins strict
  - RFID : ISO/IEC 29167-1:2014 (crypto-suites, architecture)
  - Circuits intégrés : ISO/IEC WD 19286.4 (protocols and services ensuring privacy)
  - IETF (ACE WG)…
- **Axes de recherche**
  - Solutions protocolaires (établir des communications sécurisées, non traçables)
  - Architectures de services pour l'Internet des objets (cloud, traitements confidentiels, intègres…)
  - Fiabilité des logiciels au sein des objets (difficulté de mises à jour, intégrité)

Solutions protocolaires

- **Protocoles de sécurité**
  - Bootstrapping de la sécurité
  - Miniaturiser les protocoles de communications et de sécurité
  - Protocoles de bout en bout, routage sécurisé
  - Tenir compte du caractère vulnérable physiquement des objets
- **Protocoles de sécurité assistés par un/des nœud(x) (objet ou cloud)**
  - Pour un réseau d'objets hétérogènes dans leurs capacités
  - Répartir une partie des calculs auprès d'un ou plusieurs noeud(s)
    - Réduit les coûts de calculs sur l'objet demandeur
    - Améliore le niveau de confiance si les calculs sont distribués sur plusieurs objets
  - Problèmes : distribution de calculs et mesure de la confiance associée à un objet
- **Solutions cryptographiques**
  - Comment réduire le coût en calculs et mémoire des algorithmes de chiffrement/signature ? (Signcryption, ECC, codes correcteurs…)
  - Débat autour de la cryptographie postquantique
- **Solutions intermédiaires qui associent au plus près la cryptographie aux protocoles de sécurité**

Solution associant au plus près cryptographie et protocoles

- Objectif : un objet de faibles capacités (RFID, capteur…) s'authentifie et chiffre de faibles volumes de données
- Eléments techniques
  - Adaptation du cryptosystème à clef publique NTRU avec répartition astucieuse de la charge de calcul
  - Propriétés : Passage à l'échelle et niveau de sécurité élevé (résistant à : traçabilité, déni de service, rejeux)



Gestion de la confiance inter noeuds dans un Internet des objets ?

- **Objectifs : permettre à des objets de détecter les noeuds proxies alentour malveillants et choisir les nœuds assistants en fonction du niveau de confiance mesuré**
- **Les systèmes de gestion de la confiance**
  - En majorité, traitent la confiance service par service (radio, routage, sécurité)
  - En minorité, considèrent la diversité des services offerts par un noeud mais agrègent toutes les expériences de service en une seule métrique , ce qui dégrade la qualité de la mesure
- **Proposition d'un système de gestion de la confiance multi-service et contextuel (capacité de ressources du proxy, horodatage, âge…)**
  - Répond à la question : quel proxy vaut-il mieux sélectionner pour réaliser un service demandé ?

Gestion de la confiance : Méthode de sélection du proxy

Etape 1 : Limiter le nombre de candidats proxies Pi à ceux susceptibles de rendre le service recherché à un objet demandeur

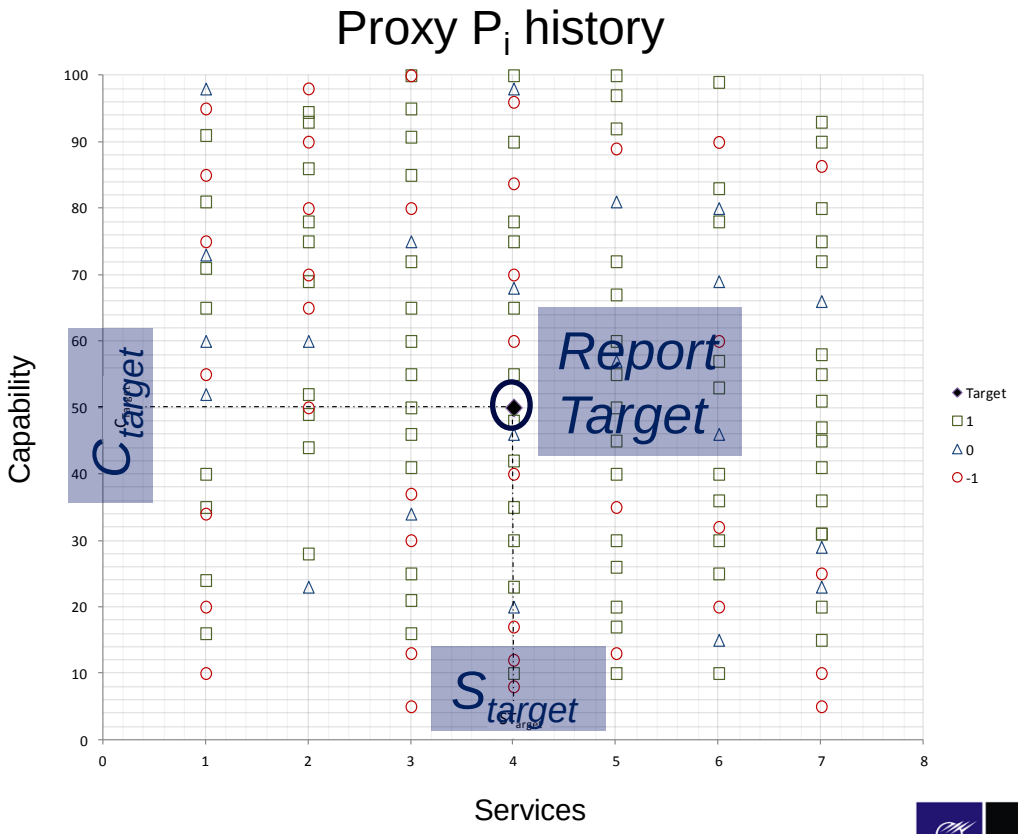
- Pour un service de sécurité, contrainte de partager une clé symétrique par exemple
- Pour un service radio, les proxies doivent nécessairement être dans la portée du nœud demandeur

Gestion de la confiance : Méthode de sélection du proxy

Etape 2 : ne conserver qu'un sous-ensemble de rapports R_{ij} pour chaque proxy

Problem : not enough reports to calculate the trustworthiness of a node in a specific context

Introduce the context similarity concept



Gestion de la confiance : Méthode de sélection du proxy

Etape 2 : ne conserver qu'un sous-ensemble de rapports R_{ij} pour chaque proxy

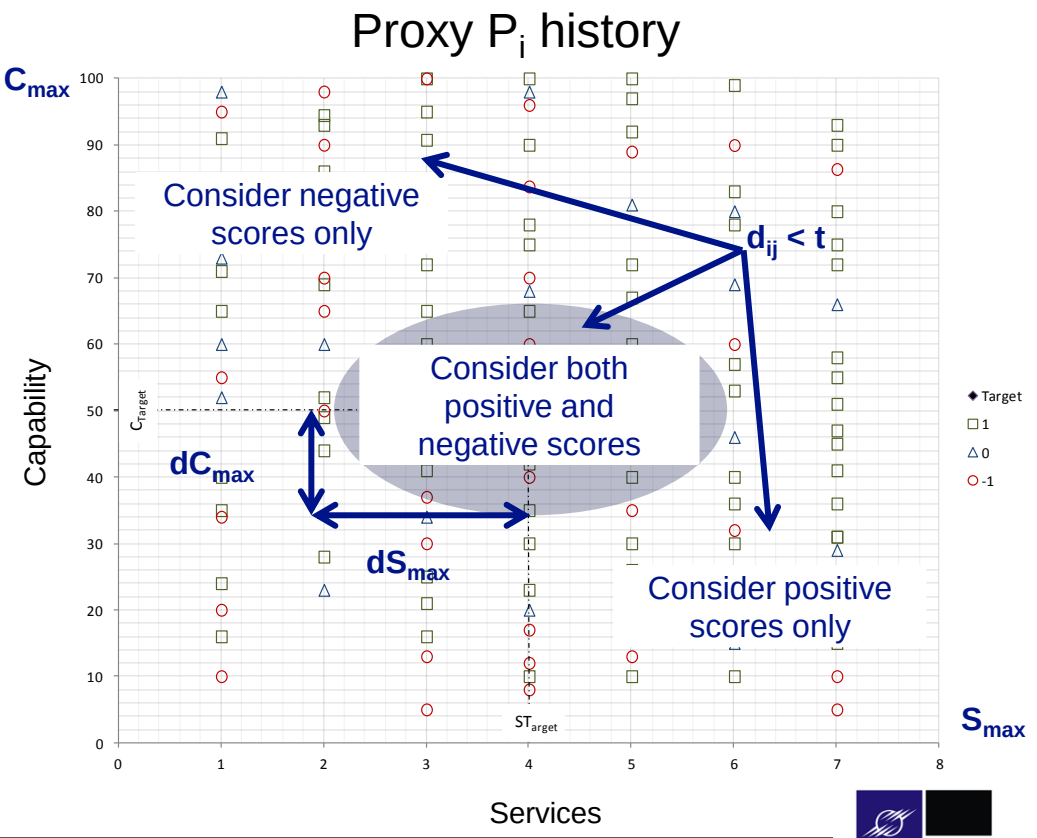
- Compute contextual distance d_{ij} :

$$dS_j = \left| S_{Target} - S_j \right|$$

$$dC_j = \left| C_{Target} - C_j \right|$$

- A retained report R_{ij} should have a distance d_{ij} (R_{ij}, R_{Target}) < t, with

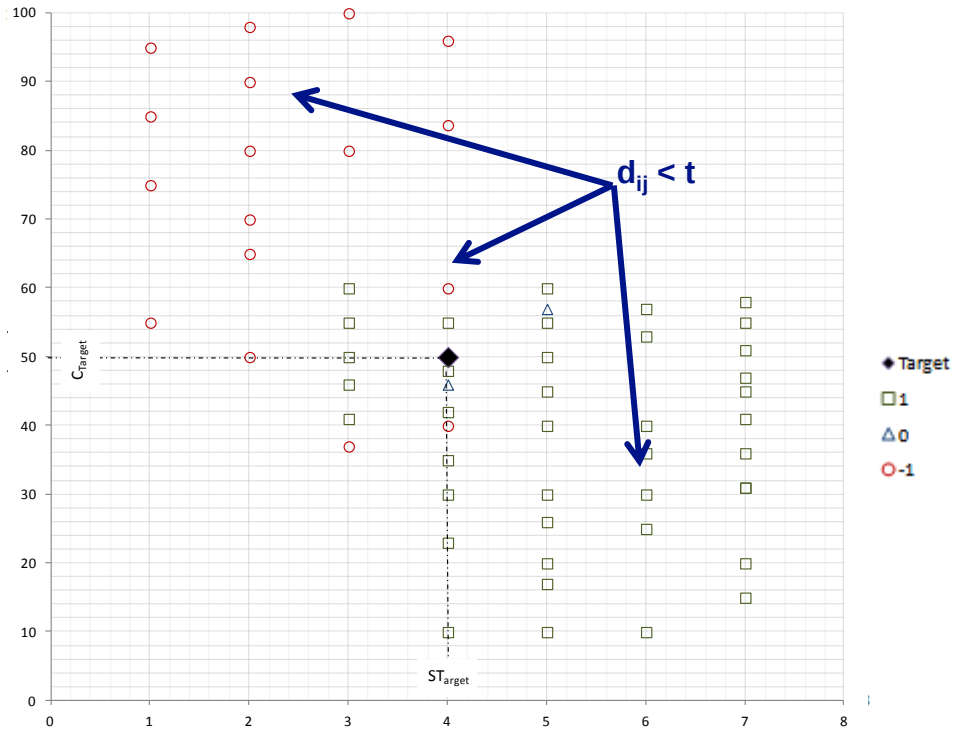
$$t = \sqrt{dS_{max}^2 + dC_{max}^2}$$



Gestion de la confiance : Méthode de sélection du proxy

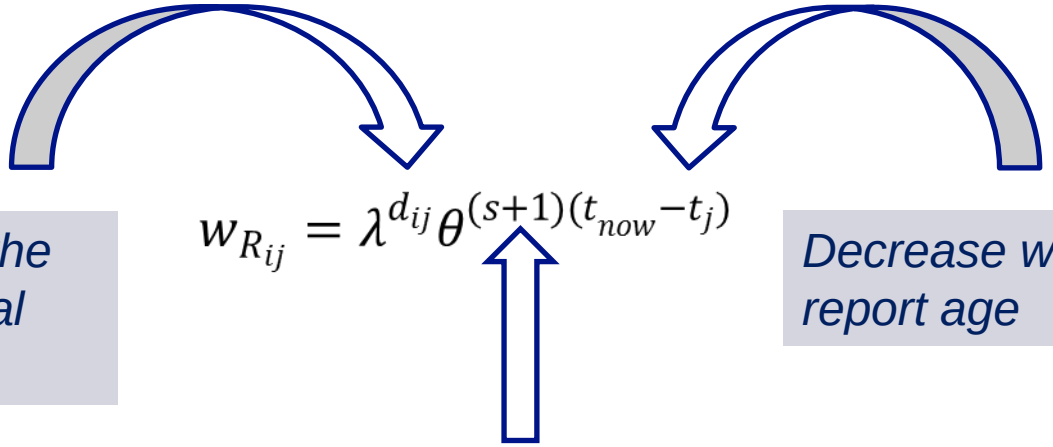
Etape 2 : ne conserver qu'un sous-ensemble de rapports R_{ij} pour chaque proxy

Retained reports for proxy P_i



Gestion de la confiance : Méthode de sélection du proxy

Etape 3 : Calcul des poids de chaque rapport retenu



$$w_{R_{ij}} = \lambda^{d_{ij}} \theta^{(s+1)(t_{now} - t_j)}$$

Decrease with the report contextual distance

Decrease with the report age

$s = {}^{1}/_{2} * (N_j{}^2 - N_j)$

make negative scores appear less old

Gestion de la confiance : Méthode de sélection du proxy

Etape 4 : Calcul du niveau de confiance T_i pour chaque proxy P_i

$$T_i = \frac{1}{\sum_{j=1}^{n} w_{R_{ij}}} \times \sum_{j=1}^{n} (w_{R_{ij}} . QR_j . N_j)$$

Report weighting factor computed in step 3

Score assigned in the report R_{ij} to evaluate the proxy P_i

Quality of recommendation of the reporting node

Ces travaux prennent place au sein de…

- **Action « Objets Intelligents et Internet des objets »**
  - Action du CNRS rassemblant industriels et académiques
  - Coanimatrices : M. Laurent (TSP) et S. Bouzefrane (CNAM)
  - Thèmes : Plate-formes de confiance, RFID, NFC, TEE, Sécurité, Protection des données personnelles, Confiance numérique, Objets communicants
  - Objectifs: regrouper la communauté française travaillant sur cette thématique, organiser des événements scientifiques, créer un club de partenaires industriels
  - **Evènement du 17 juin 2015, CNAM, Paris : « Internet des objets et cybersécurité/cyberdéfense »**

- **Chaire Institut Mines-Télécom Valeurs et politiques des informations personnelles**
  - 1ère chaire de l'Institut Mines-Télécom
  - Chaire multidisciplinaire (juridique, technique, économique, sociale, et éthique)
  - Mécènes : Imprimerie Nationale, BNP Paribas, Orange, LVMH, Dassault Systèmes, Deveryware, en partenariat avec la CNIL
  - Objectifs : aider les entreprises, les citoyens et les pouvoirs publics dans leurs réflexions sur la collecte, l'utilisation et le partage des informations personnelles, à savoir les informations concernant les individus (leurs vies privées, leurs activités professionnelles, leurs identités numériques, leurs contributions sur les réseaux sociaux, etc.) incluant celles collectées par les objets communicants qui les entourent (*smartphones*, compteurs intelligents, télévisions connectées ou jouets intelligents de type NFC, etc.)
  - http://cvpip.wp.mines-telecom.fr/

L’équipe de recherche pluridisciplinaire

Maryline Laurent

Professeur en sciences de l’informatique

Patrick Waelbroeck

Maître de conférences en sciences économiques

Pierre-Antoine Chardel

Professeur en philosophie

Claire Levallois-Barth

Maître de conférences en droit

et les ressources STIC de l’Institut Mines-Telecom

Les cinq axes de recherche de la chaire

- Identités numériques
- Gestion des informations personnelles
- Contributions et traces
- **Informations personnelles dans l'Internet des objets**
- Politiques des informations personnelles

1. Régulation juridique, propriété des identifiants
2. Co-responsabilités juridique et éthique
3. Traçabilité, anonymisation
4. Gestion et sécurité des flux automatisés, dont *cloud*

Références

- **Ouvrage**
  - "La gestion des identités numériques", (Ed. M. Laurent, S. Bouzefrane), collection ISTE, ISBN: 978-1-78405-056-6 (papier), ISBN : 978-1-78406-056-5 (ebook), 2015.
- **Publications personnelles**
  - K. Nguyen, M. Laurent, N. Ouahla, “Survey on Secure Communication Protocols for the Internet of Things”, Ad Hoc Networks Journal (Impact Factor: 1.94), Feb. 2015; DOI: 10.1016/j.adhoc.2015.01.006.
  - Y. Ben Saied, A. Olivereau, M. Laurent, D. Zeghlache, “A Survey of Collaborative Services and Security-related Issues in Modern Wireless Communications”, Journal of Network and Computer Applications, 2014.
  - Y. Ben Saied, A. Olivereau, D. Zeghlache, M. Laurent, “Lightweight collaborative keying for the Internet of Things”, Elsevier Computer & security, 2014.
  - Y. Ben Saied, A. Olivereau, M. Laurent, “A Distributed Approach for Secure M2M Communications”, International Conference on New Technologies, Mobility and Security NTMS 2012, May 2012, Istanbul, Turkey.
  - Y. Ben Saied, A. Olivereau, D. Zeghlache, M. Laurent, “Trust management system design for the Internet of Things: A context-aware and multi-service approach”, Computers & Security, 2013.
  - E. El Moustaine, M. Laurent, “ Procédé pour crypter des données dans un cryptosystème NTRU (N,p,q) ”, numéro le n° PCT/IB2013/055122, 2013.
- **Références juridiques**
  - Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE n° L 281 du 23 novembre 1995.
  - Groupe Article 29, *Opinion 8/2014 on the on Recent Developments on the Internet of Things, a*dopted on 16 September 2014, WP223.
  - NF EN 16571, « Technologies de l'information - Processus d'évaluation d'impact sur la vie privée des applications RFID », Juillet 2014.
- **Références/publications techniques**
  - ISO/IEC 29167-1:2014, “Information technology -- Automatic identification and data capture techniques -- Part 1: Security services for RFID air interfaces”, Août 2014.
  - ISO/IEC WD 19286.4, “Identification cards — Integrated circuit cards — Protocols and services ensuring privacy”, Working Draft, 2015
  - ITSEC (Information Technology Security Evaluation Criteria), “Information Technologie System Evaluation Criteria “, 1991