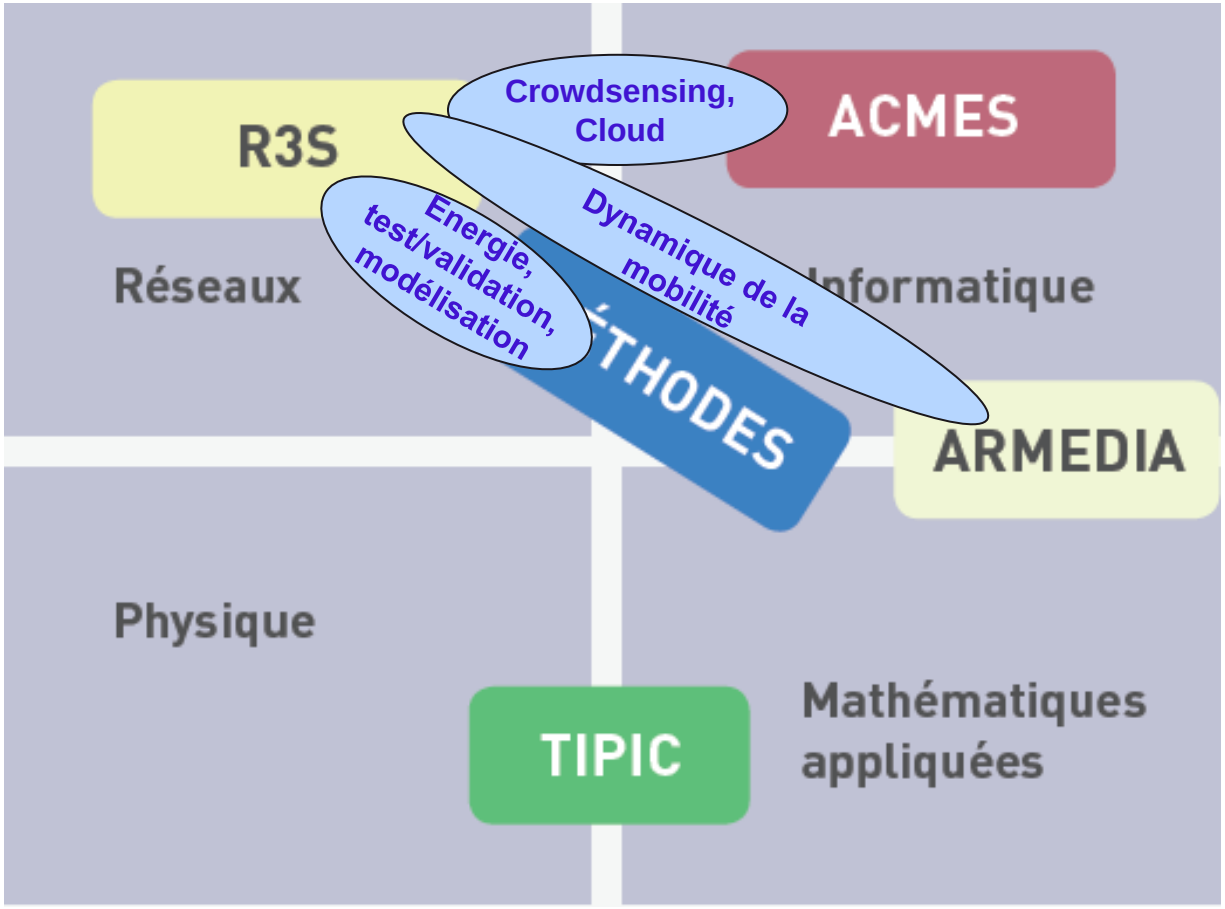
Evaluation de l'unité SAMOVAR UMR 5157
5 décembre 2018

Bilan et projet de l'équipe R3S
Réseaux, Systèmes, Services, Sécurité

Maryline Laurent

Positionnement de R3S dans SAMOVAR



Membres de l'équipe (1er janvier 2018)

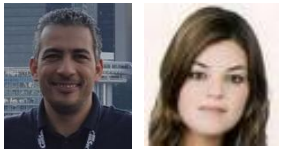
- **17 enseignant-chercheurs**

Axe RS
Réseaux et Services

Axe SSR
Sécurité des Systèmes et des Réseaux

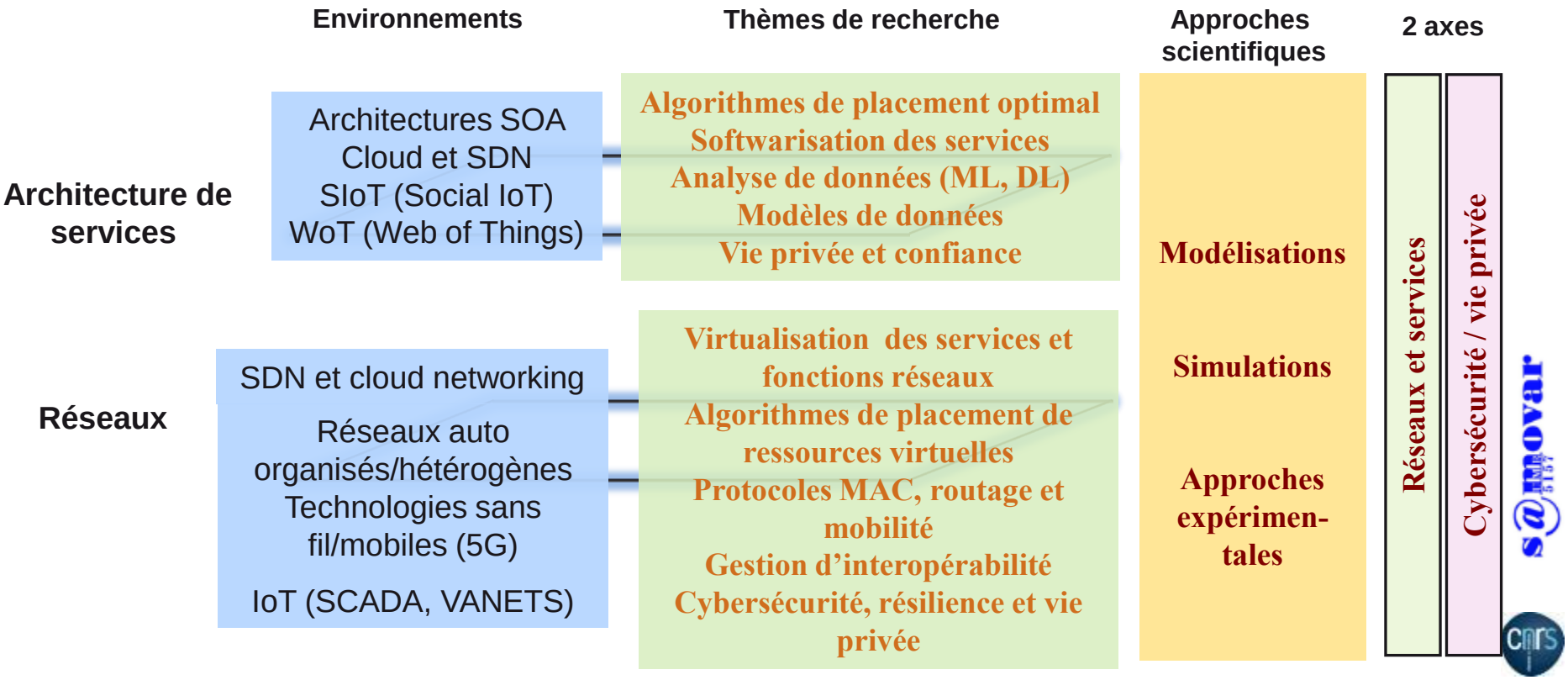
- **1 ingénieur**

2 chercheurs associés



- **36 doctorants, 1 post-doctorant, 18 chercheurs/ingénieurs (CDD), et 1 ingénieur plateforme**

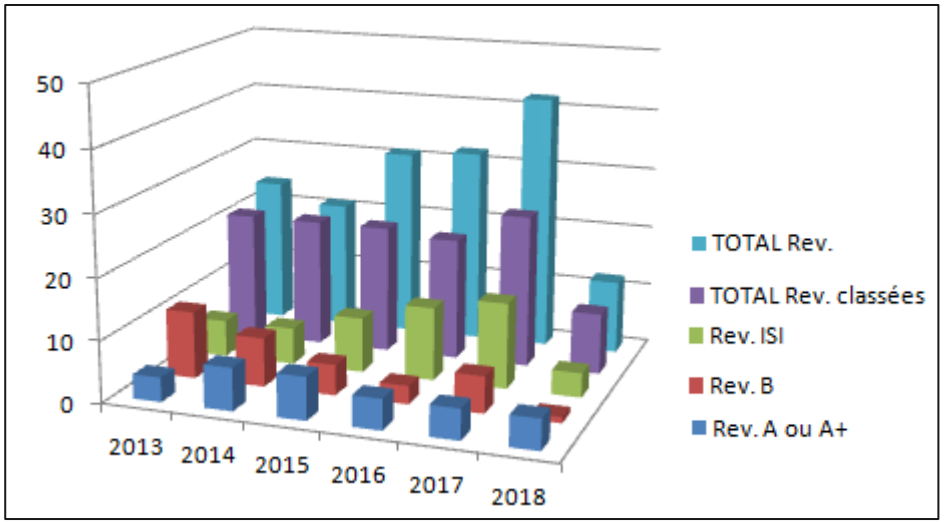
Compétences de l'équipe



Domaines d'intérêt majeurs de l'IMT : Industrie 4.0, Energie, Smart cities et Transports

Années thématiques du CNRS : Sécurité et Objets communicants

Activités scientifiques et bilan



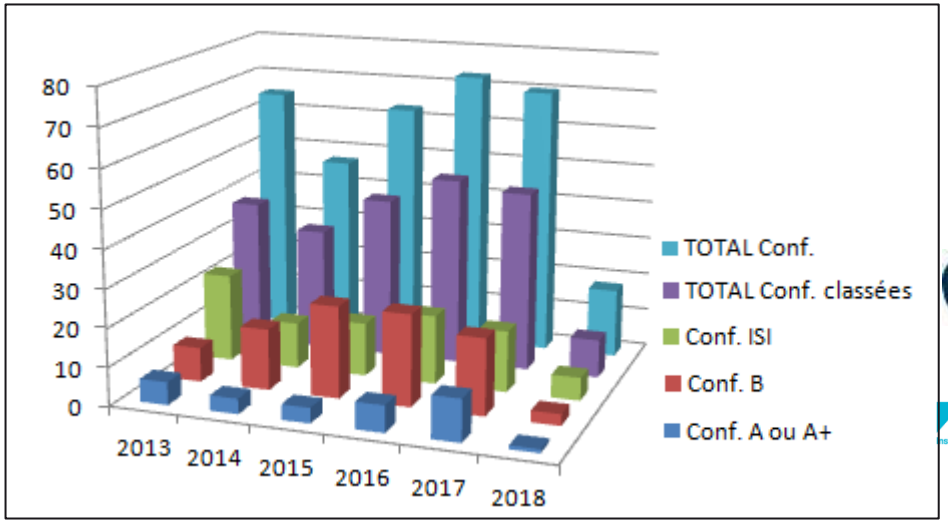
162 articles de revues

- **73% revues classées**
- **2 articles / permanent / an en moyenne**

336 articles de conférences

- **65% en conférences classées**
- **+26% d'articles en conférences classées (2013-2017)**

7 prix du meilleur article
4 logiciels (github), 4 prototypes, 3 bases de données
5 plateformes
4 séjours invités dans des laboratoires à l'international
Citations (+500 pour un survey sur IoT)
10 ouvrages scientifiques (+25000 téléchargements de chapitres)
Livre blanc (5G) classé no5 en popularité pour IEEE Institute en 2016

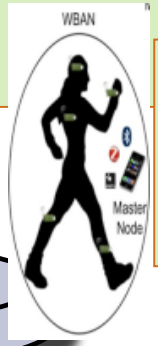


Bilan : Réseaux et services

LTE
- Communications de groupes (multicast) sur LTE – optimisation des ressources et de l'efficacité énergétique [23.C.rs, Best paper award]
- Service de voix sur IP – Ordonnanceur [16.J.rs]

LTE : Long Term Evolution

Réseaux sans fil/mobiles
Réseaux auto-organisés



WBAN : ontologie – meilleure interopérabilité des services WBAN [23.J.rs]
Standardisation ETSI SmartBAN

WBAN : Wireless Body Area Network

VANETs :
- 3 protocoles d'accès au canal, pour les réseaux VANETs, s'appuyant sur TDMA – réduction des délais d'acheminement [36.C.rs, 35.C.rs, 50.C.rs]
- Modélisation du nombre de sauts dans un réseau V2V – pour tout profil de trafic routier – nombre de clients dans une file à arrivées dépendantes et temps de service constant [24.J.rs]

TDMA : Time Division Multiple Access
V2V : Vehicule to Vehicule

Bilan : Réseaux et services

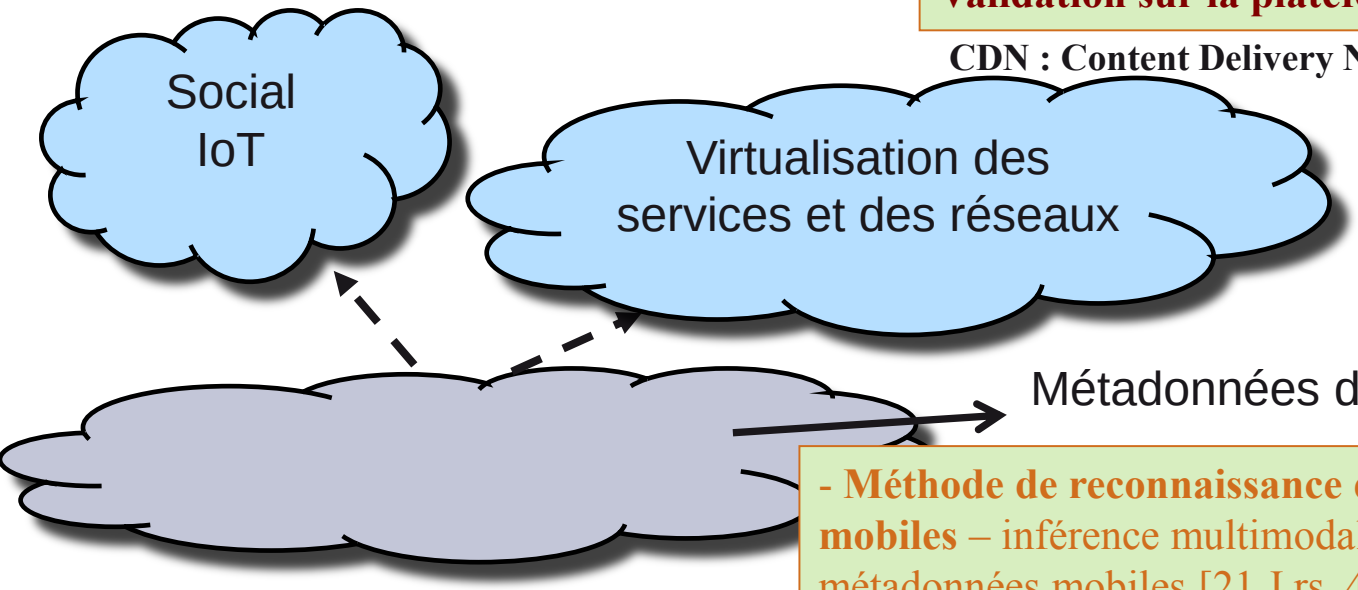
- **Framework de virtualisation des objets en soutien au SIoT** [25.C.rs]
- **Méthodologie de définition de la granularité des composants et de leurs intéractions dans le rendu d'un service global** [34.J.rs, 6.L.rs]

- **Orchestrateur de services reposant sur le framework TOSCA étendu à des notions de réseau** [10.J.rs, 30.C.rs]
- **Test et validation de services par des modèles avant déploiement** [20.J.rs, 13.C.rs]
- **Fournisseur de caches virtuels pour CDN** [12.J.rs]

(collaborations avec l'équipe METHODES)
Validation sur la plateforme Cloud et réseaux

SIoT : Social IoT

CDN : Content Delivery Network



- **Méthode de reconnaissance de trajectoires mobiles** – inférence multimodale, uniquement sur des métadonnées mobiles [21.J.rs, 4.O.rs]

(collaboration avec ACMES et ARMEDIA)

Bilan : Sécurité des systèmes et réseaux

- Framework de lutte contre les attaques DDoS – contrôleur SDN enrichi [6.J.rs, 44.C.rs]
- Formalisation de la migration de topologies virtuelles avec maintien des propriétés de sécurité [24.C.rs]
Validation sur la plateforme THD-SEC

DDoS : Distributed Denial of Service
SDN : Software Defined Networking

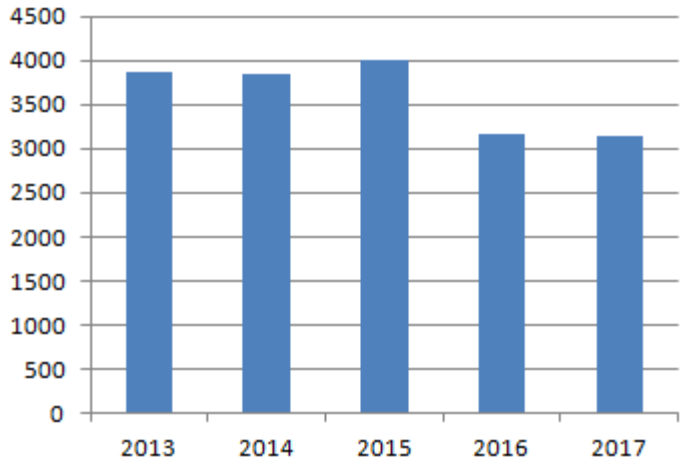
Virtualisation des réseaux – SDN

Résilience des CPS - détection d'erreurs (industrie) étendue aux cyberattaques et réaction par SDN [7.J.rs, 8.J.rs, 27.C.rs]
Validation sur la plateforme THD-SEC
Chaire Cyber CNI

CPS : Cyber Physical System

- Externalisation des calculs cryptographiques d'un objet sans perte de sécurité/vie privée – semi-trusted model [4.J.rs, 29.C.rs]
- Modèle de gestion de la confiance – contexte, réputation et capacité des nœuds [35.J.rs]
Chaire VPIP

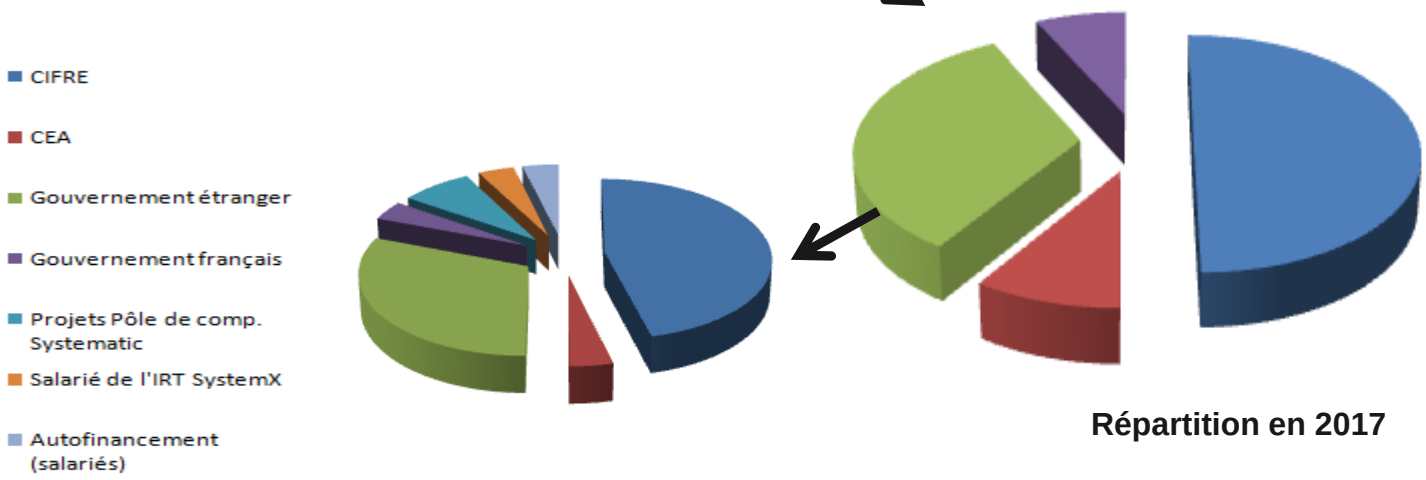
Activités de valorisation et de transfert



Evolution des ressources (en k€)

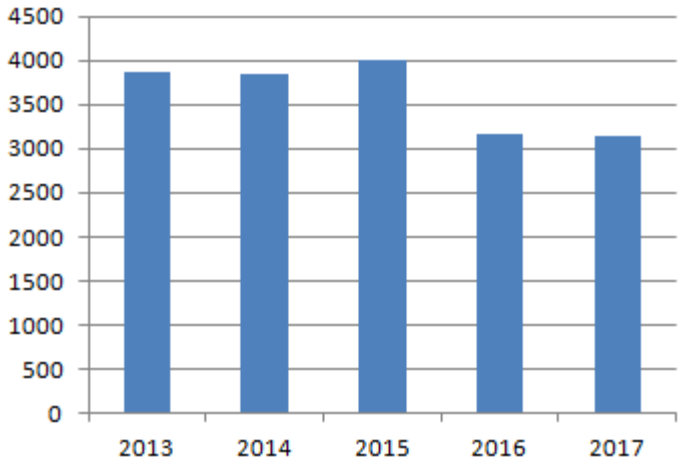
2,6 millions € / an en moyenne
(projets européens et nationaux)

Effort de diversification pour pallier au fléchissement des recettes
(PIA, mécénat, ~30 bourses de thèse/an dont ~15 CIFRE/an)



Répartition en 2017

Activités de valorisation et de transfert

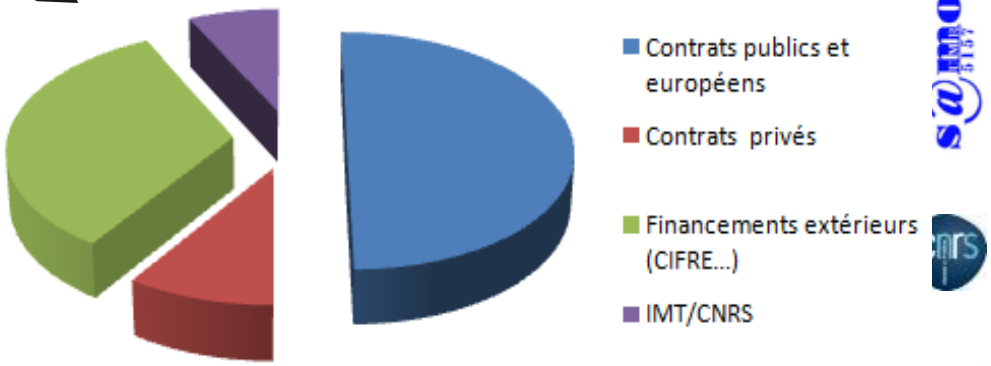


Evolution des ressources (en k€)

2,6 millions € / an en moyenne
(projets européens et nationaux)

Effort de diversification pour pallier au fléchissement des recettes
(PIA, mécénat, ~30 bourses de thèse/an dont ~15 CIFRE/an)

~15 projets européens (4 pilotés)
2 chaires de l'IMT dont une multidisciplinaire
Nombreux partenaires industriels
3 brevets (acceptés)
1 laboratoire commun avec EDF (SEIDO)
Standardisation (ETSI, OneM2M, AIOTI, ITU-T)
PPP ECSO et consultations nationales
Diffusion grand public (radio, TV, presse)



Répartition en 2017

Formation par la recherche

- 106 doctorants (62 ayant soutenu), 26 postdoctorants et 85 chercheurs/ingénieurs (CDD)
- Contribution aux masters de Paris-Saclay :
  - Montage de 3 masters/parcours
  - Coordination du M1 Computer Science (International Track)
  - ~10 modules de cours de masters coordonnés (M1 et M2)
- Elaboration de MOOCs
  - Programmer l'Internet des objets
  - Théorie des files d'attente
  - A la découverte des télécommunications
  - Supervision de réseaux
- Ecole thématique "Secure Smart objects&The IoT" organisée dans le cadre du GDR ASR

Appui à la communauté

- **Organisation de plus de 10 conférences dont la 19 ème édition de la conférence en sécurité RAID 2016 à Evry**
- **Comités éditoriaux de journaux Computers&Electrical Engineering, Computers&Security… et éditeurs de numéros spéciaux associés à World Wide Web, Security and Computers Electrical Engineering...**
- **Comité de pilotage de conférences / Animation de journées scientifiques (Energie, IoT, Cybersécurité, Confiance)**
- **Expert H2020, évaluations de projets ANR**

Analyse SWOT

Points forts

- Très bonne visibilité nationale et internationale
- Croissance des collaborations internationales/nationales et inter équipes/labos
- Engagement fort auprès des instances européennes et nationales
- Forte capacité à innover
- Sources de financement diversifiées

Points faibles

- Manque d'ingénieurs (hors contrat)
- Collaborations inter et intra équipe à renforcer

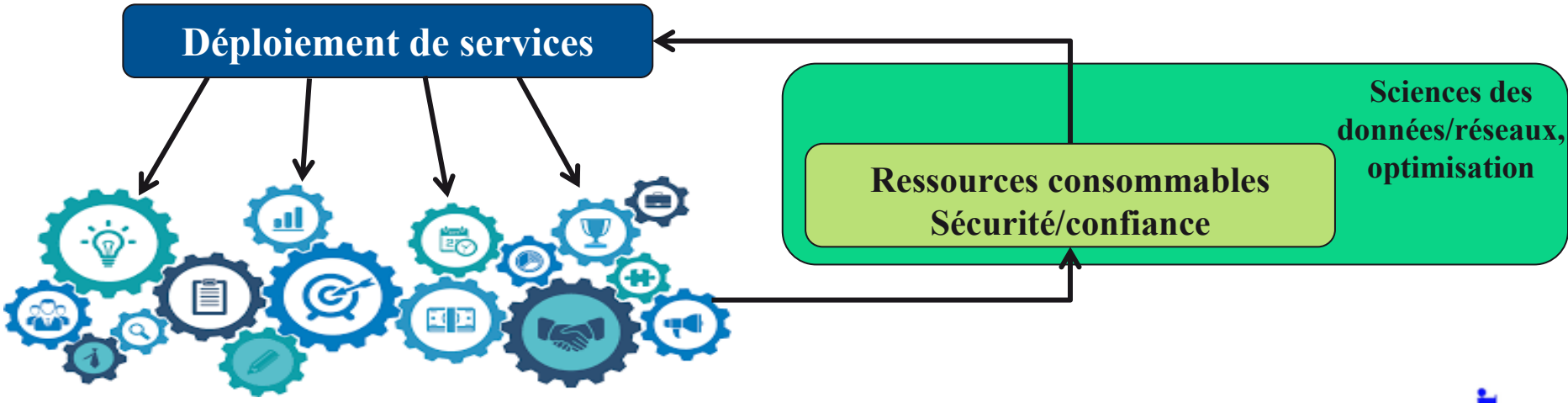
Opportunités

- Opportunité liée à l'intégration dans NewUni et son écosystème « sciences des données » et « sécurité »

Risques

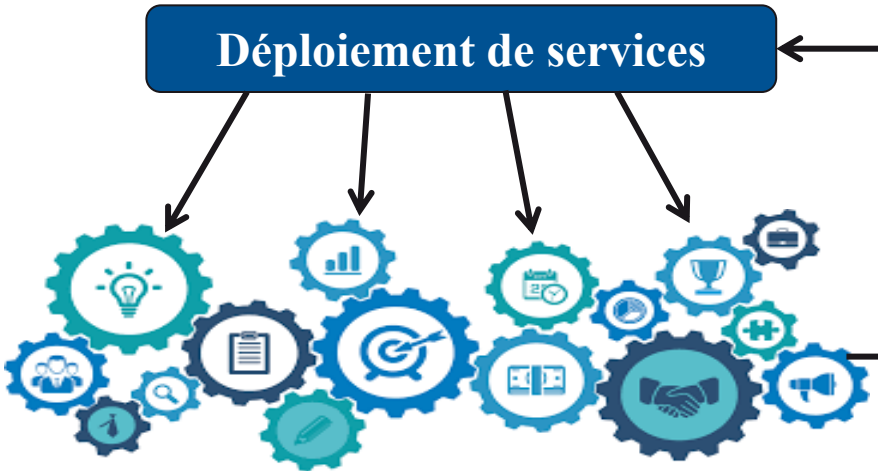
- Bilocalisation
- Financements

Projet 1 : Optimisation de ressources pour des services sous contraintes



- Ajustement continu et rétroactif du déploiement de services
- Verrous : passage à l'échelle des techniques de traitement de données, hétérogénéité des données et des technologies supports

Projet 1 : Optimisation de ressources pour des services sous contraintes



7 membres R3S impliqués dont 3 SSR et 4 RS

- 3 cas d'usage considérés :
  - **Les services virtualisés (QoE et ressources) : besoins de prédiction de la demande, détection d'anomalies/dégradations**
  - **La sécurité (sécurité des clients et opérateurs) : besoins de détection des incidents, de maintien de la sécurité/résilience**
  - **Les réseaux électriques (stockage de l'énergie) : besoin de prédire et coordonner la consommation/production d'énergie**

Projet CELTIC SENDATE
Collaborations avec Nokia, Thalès

Projet DATAIA PEPER
Collaboration avec les laboratoires GEEPS et LMD

Projet 2 : Sécurité et protection des donnés personnelles dans le cas d'applications critiques

- Architecture reposant sur des capteurs, actionneurs, contrôleurs et cloud

- Besoins : résistance aux attaques, résilience, sûreté de fonctionnement, conformité RGPD, interopérabilité, personnalisation de services
  - E-santé : ergonomie, automatisation, traçabilité des acteurs
  - Industrie 4.0 : propriété intellectuelle
- Verrous : ressources limitées, environnement ouvert/dynamique

Projet 2 : Sécurité et protection des donnés personnelles dans le cas d'applications critiques

7 membres R3S impliqués dont 5 SSR et 2 RS

- **Méthodes envisagées :**
  - **apprentissage profond (détection d'anomalies)**
    - Collaboration avec le Japon
  - **couplage sécurité/confiance ou programmabilité des réseaux SDN (isoler un attaquant)**
    - Chaire Cyber CNI
  - **mode dégradé (résilience)**
    - Chaire CNI
  - **ontologies à aligner et analyse sémantique (interopérabilité)**
    - Standardisation ETSI au sein du comité technique SmartM2M (workshop Smart BAN coorganisé durant l'ETSI IoT Week 2018, présentation d'un showcase oneM2M)
    - Collaboration avec l'Université Libanaise
  - **fonctions cryptographiques légères (personnaliser un service)**
    - Chaire CVPIP
  - **preuves cryptographiques (gestion du consentement à la RGPD)**
    - Collaboration avec ACMES
- **Instruments en soutien démarrés en 2018-2019 :**
  - **Réseau d'excellence H2020 SPARTA piloté par CEA (resp. IMT : R3S)**
  - **Thématique phare IMT "Risques et cybersécurité" (copilotée par R3S)**
  - **Thématique phare IMT "Réseaux et IoT" (copilotée par R3S)**

L'équipe R3S vous remercie

et vous invite à découvrir leurs posters/démos

- Multi-provider Slice Embedding under Security Constraints **Démo**
- Prédiction de la prosommation d'énergie renouvelable par apprentissage **Démo**
- Studying information Dissemination in D2D Network using Call De
- Blockchain based trust management mechanism for Industry 4.0
- More recent results on slice extension algorithms **Démo**
- ETSO: End-To-End SFC Orchestration Framework Addressing NFV Challenges
- Formal Approaches for Testing in Software Defined Networks
- ETSI Smart BAN specifications and standards based IoT platform (one M2M-based) for elderly at home monitoring and support
- SEAS ITEA3 project Smart Energy Aware Systems - The energy world of tomorrow **Démo**
- Validating and Repairing Virtual Service Requests (R3S-METHODES) **Démo**
- Modeling and performance evaluation of the eICIC/ABS in H-CRAN (R3S-METHODES)

- Cyber-Physical Security Training Platform **Plateforme**