Projet : SENSAI

SEnsor Network Security through Artificial Immune systems

Coordinateur du projet : Parrend Pierre

ICube, Université de Strasbourg, CNRS

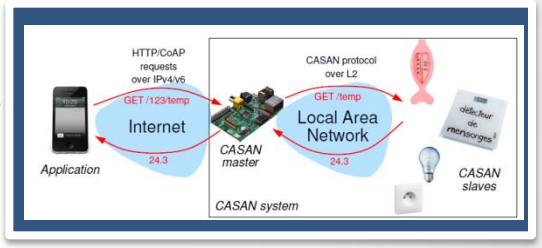
API 2015

Projet : acronyme

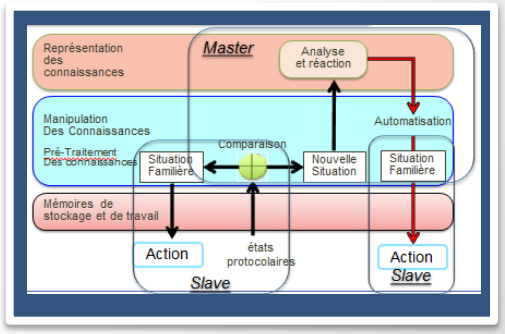
Résumé du projet

- **Résumé :**

Les réseaux de capteurs ont comme caractéristique de rassembler des nœuds disposant de ressources très contraintes en termes de puissance processeur, de mémoire et d'énergie. Leur mise en œuvre réelle passe par la prise en compte de la problématique de la sécurité, c'est-à-dire la protection vis-à-vis de comportements malveillants tels qu'une intrusion, ou accidentels tels qu'une défaillance, pouvant altérer le fonctionnement du réseau lui-même.



Dans SENSAI, nous caractériserons les vulnérabilités de sécurité des réseaux de capteurs à l'exemple du protocole CoAP (Constrained Application Protocol), et mettrons en œuvre un système immunitaire artificiel capable d'identifier les anomalies de sécurité et d'y répondre à la fois par le biais d'une réaction primaire – « comment traiter une nouvelle anomalie ? » – et secondaire – « comment réagir à une anomalie connue ».



- **Mots clés :** sécurité, réseaux de capteurs, systèmes immunitaires artificiels

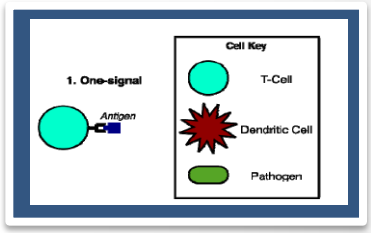
Projet : acronyme

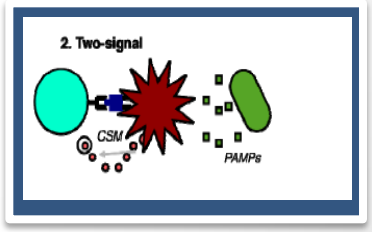
Problématiques scientifiques

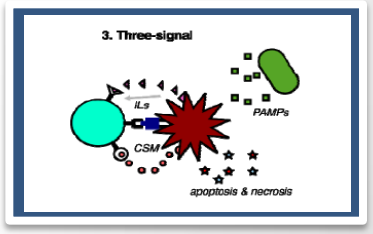
- **Objectifs scientifiques**
  - Analyse, conception et réalisation d'un **système immunitaire artificiel** pour les réseaux de capteurs à l'exemple de **CoAP (Constrained Application Protocol)**

- **Approche envisagée**
  - **Phase 1: caractérisation des anomalies propres au protocole CoAP, algorithme de détection d'anomalies de sécurité**
  - **Phase 2: système immunitaire artificiel,** application d'**analyse de sécurité** et de **réaction aux attaques**

- **Originalité**
  - **Définition et la conception d'un système immunitaire artificiel capable de caractériser le niveau de confiance** sur la base d'un **minimum d'informations**,
  - **Réaction** en conséquence







Projet : SENSAI

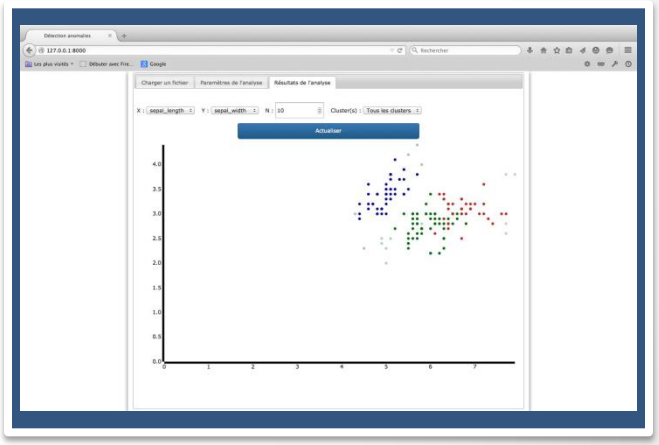
Participants

- **Nom(s) du ou des coordinateurs :** Parrend Pierre, Enseignant-Chercheur ECAM Strasbourg-Europe, équipe BFO
- **Noms des participants :** Pierre David (McF), Guillaume Schreiner (IR), Philippe Pitolli (Master Réseaux), Paul Cardosi (Master ILC), Fabio Guigou (Doctorant Cifre)
- **Équipes impliquées :** Réseaux; BFO
- **Axes transverses concernés :** Calcul scientifique et fouille de données (CS)
- **Complémentarité des participants :** pour répondre à l'enjeu de **sécurité de l'Internet des Objets,** l'équipe **Réseaux** joint sa forte expérience sur les réseaux de capteurs aux compétences de BFO sur la **fouille de données** et les **algorithmes bio-inspirés.**

Projet : acronyme

Résultats préliminaires

- **Stage de Philippe Pittoli (Février-Juin 2015):** caractérisation des vulnérabilité des réseaux de capteurs; identification des protections apportées par les protocoles existants
- **Implémentation** d'un premier algorithme de classification des attaques par **système immunitaire artificiel,** et d'une première version de **l'interface graphique**
- Stage de **Paul Cardosi**: démarrage sur le sujet **Octobre 2015**



- **Communications**
  - 'Failed promises and actual stakes of Artificial Immune Systems', Journée 'Evolution Artificielle Thématique', le 12/6/2015
  - An Artificial Immune Ecosystem model for hybrid cloud supervision, Fabio Guigou, Pierre Parrend, Pierre Collet, submitted to CS-DC'15