Petit point intermédiare sur l'ARC SéSur

Travaux de Nîmes/Montpellier

Travaux d'AxIS

Travaux de Montpellier (LIRMM)

- **Yoann Pitarch**
- Sujet : « Fouille de flots de données multidimensionnelles »
- cubes de flots de données
- 'tilted time' windows
- décrire l'évolution du cube au cours du temps
- détection de tendances et d’exceptions

Travaux de Montpellier (LIRMM)

- **Hassan Saneifar**
- Sujet : « Exploitation des connaissances textuelles pour la détection d'intrusion »
- Distance entre séquences pour le clustering des comportements passés
- Clustering des nouvelles séquences et comparaison avec l'existant (anomalies).
- Utilisation du flou : « Nombre de connexion 'élevé' sur une période 'courte' ».

Travaux d’AxIS

- **Wei Wang**
- Co-encadrement : Dream + AxIS
- Présentations d'aujourd'hui ;-)

Travaux d'AxIS (« hors ARC »)

- **Céline Fiot**
- Post-doc « en parallèle » co-encadré avec le LIRMM (TATOO)
- Extraction de tendances dans les données
- découverte de co-evolutions, ne suivant pas nécessairement la même tendance, dans des bases de séquences

Travaux d'AxIS (« hors ARC »)

- **Céline Fiot**
- Motifs d'évolution :

« Une augmentation du nombre de requêtes à la page registration.php sur une courte période précède une diminution lente du nombre de requêtes à la page faq.html, après une très courte période »

Travaux d'AxIS (« hors ARC »)

- **Céline Fiot**
- Ted & Eva (FuzzIEEE, IPMU, Inforsid).
- Suite : clustering des profils basés sur des motifs d'évolution
- Suite (bis) : détection d'anomalies sur la base de ces profils

Travaux d'AxIS (« hors ARC »)

- **Goverdhan Singh**
- Stagiaire (Jaipur, Inde) co-encadré avec le LGI2P
- Financement Color
- Détection d'anomalies partagées par plusieurs serveurs
- Améliorer la définition de la frontière entre anomalie et attaque
- Aborder les aspects « privacy »

Travaux d'AxIS (« hors ARC »)

- **Gaurav Panthari**
- Stagiaire (Jaipur, Inde) co-encadré avec le LGI2P
- Financement Color
- Détection de motifs séquentiels fréquents sur une période précise
- Utiliser ces motifs comme anomalie potentielle ?