sentryo

CYBERSECURITY FOR THE INDUSTRIAL INTERNET

Développement d'outils de Machine Learning pour la détection d'attaques en milieu industriel

Projet TIAKI

contact@sentryo.net | www.sentryo.net

Qui sommes-nous ?

Sentryo

- Cybersécurité pour l'internet industriel

Sentryo ICS CyberVision

- Capture 100% passive de réseau
- Capacité de DPI industriel
- Cartographie et supervision de sécurité

Sentryo Security Team

- Veille sur la menace
- R&D de nouvelles techniques de détection d'intrusion
- Analyse de PLC

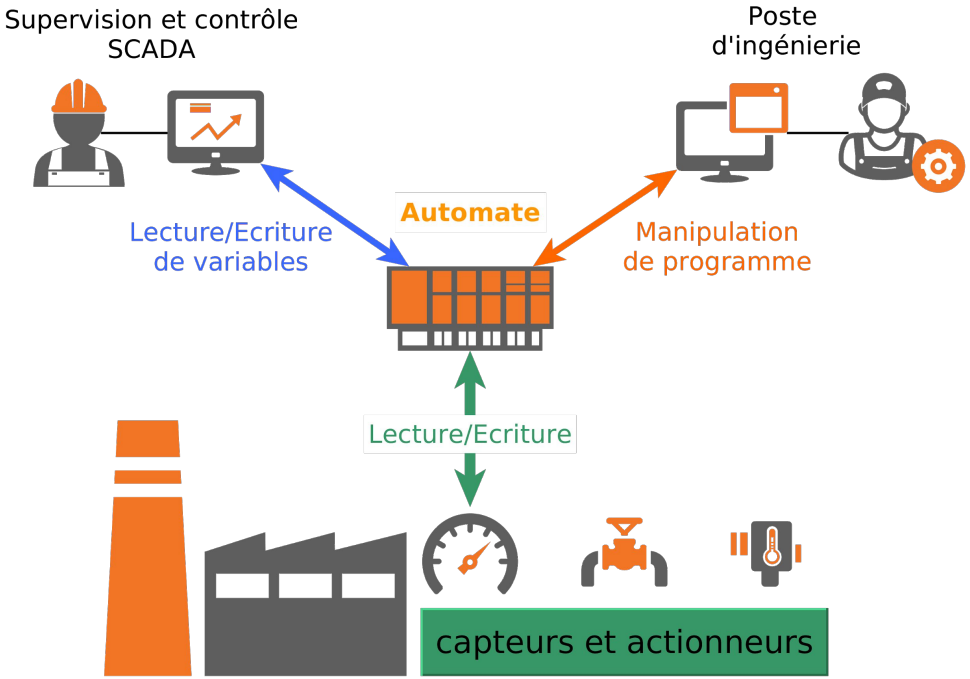
Tiaki

- Projet RAPID de 24 mois : DGA-MI/CEA-DEN/Sentryo

- Objectif : Détecter des attaques sur les réseaux industriels en utilisant des algorithmes comportementaux
  - Définition des scénarios d'attaques et de la plateforme de démo
  - Développement d'algorithmes de détection et de visualisation
  - Expérimentations

- Expérimentations réalisées sur des plateformes de test et des plateformes critiques en production

Introduction aux ICS



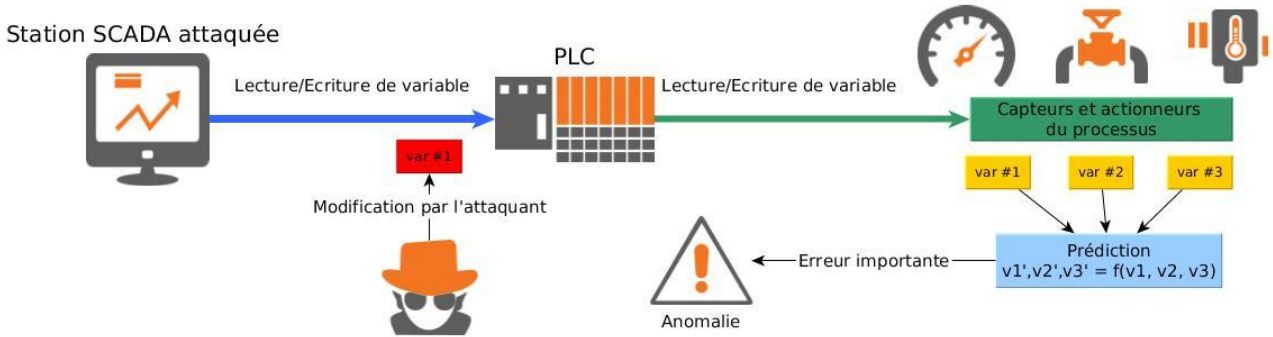
Tiaki

- Plateformes :
  - CEA : Une plateforme en production, une plateforme de test
  - Sentryo : Petits environnements de test
- Attaques :
  - Scan de ports
  - Scan de registres
  - Modification de registres et de processus
  - Téléchargement d'un programme tiers
  - ...
- Captures :
  - Captures sur les différentes plateformes du CEA. Réalisation des attaques sur la plateforme de test
  - Simulation et rejeu des attaques sur d'autres plateformes pour la portabilité

Suivi de variables

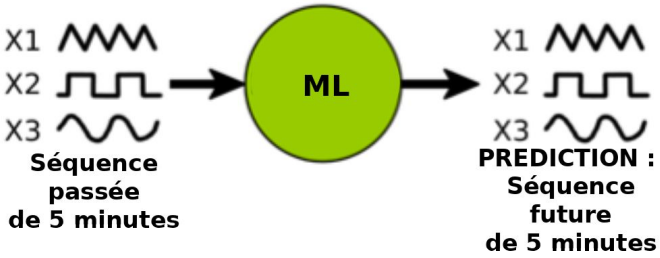
La détection d'anomalies est appliquée aux valeurs des variables d'automates. Pour apprendre la normalité, un modèle cherche à prédire les valeurs.

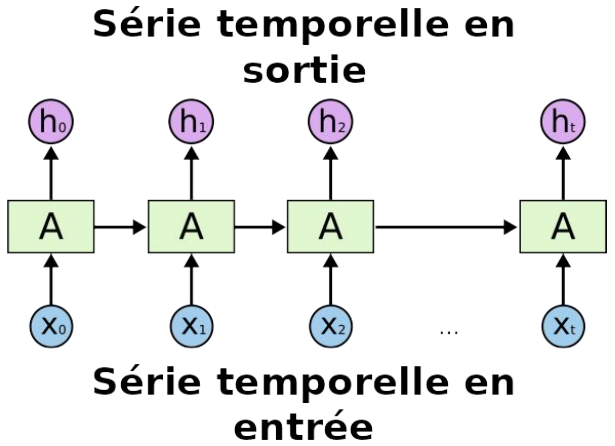
- Les valeurs sont capturées sur le réseau, via des sondes
- Un réseau de neurones prédit les valeurs suivantes
- Les prédictions sont comparées aux valeurs réelles



Description de l'algorithme

- A partir d'une fenêtre d'observation, prédire l'évolution future des mêmes variables
- Taille de la fenêtre : 100 pas de temps (5 minutes)
- Réseau de neurones récurrents (RNN) pour effectuer le mapping entre séquences passées et futures
- Prend en compte l'évolution temporelle et la corrélation entre variables
- Implémentation via Keras + TensorFlow





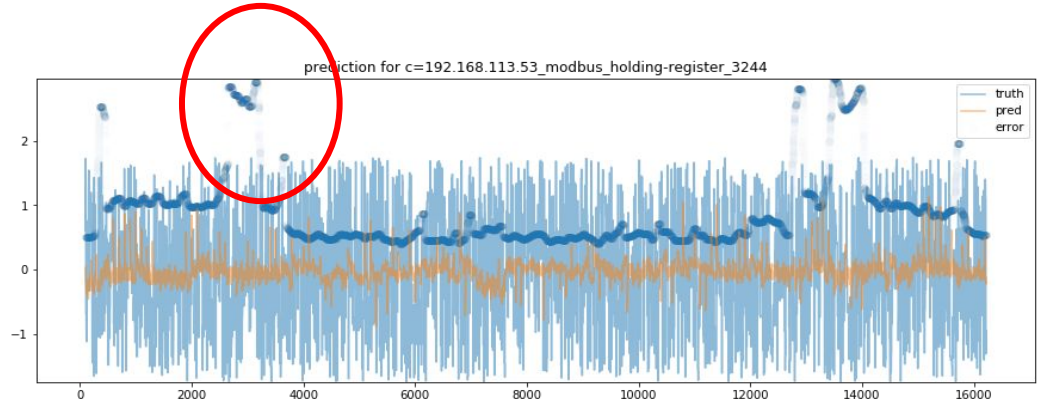
Expérimentations avec CEA Cadarache

- Journées d'évaluation à Cadarache de l'algorithme de suivi de variables
  - Captures massives (50 et 80 Go)
  - Processus inconnu
  - Puissance de calcul limitée (laptop core i7 + CG NVIDIA)

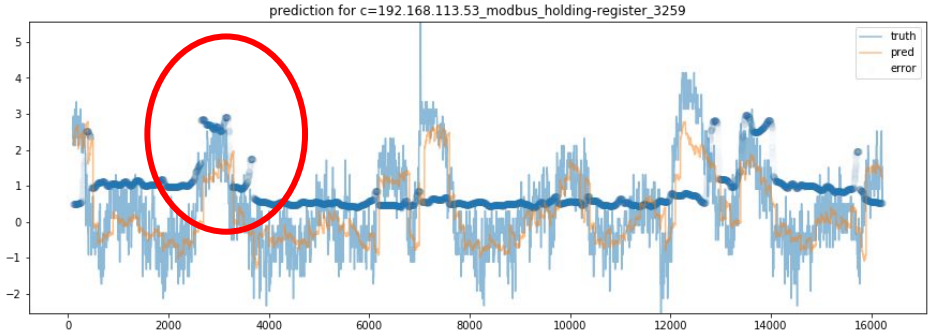
- Pré-traitement des données
  - Sélection d'un équipement et d'un protocole
  - Limitation de la taille de la capture

Résultats CEA Cadarache

- Choix automatique de variables : 134 initialement → 44 choisies
- Phases d'anomalie identifiées
- Certaines variables non informatives



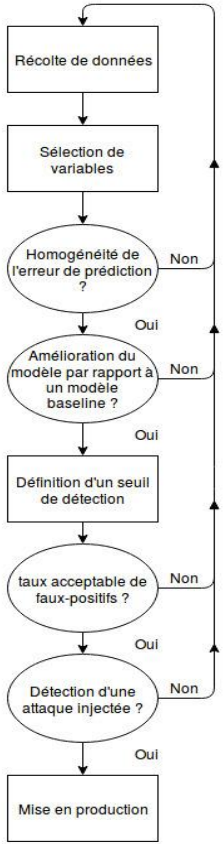
- Enseignements:
  - L'algorithme a bien détecté une phase de maintenance du process
  - Plus de traitement pour le choix de variables



Industrialisation

- Problématique de mise en service sur des plateformes critiques
  - Pas d'accès aux données
  - Pas d'accès à la solution
  - Obligation de performances

- Développement d'un superviseur
  - Automatisation des tâches
  - Vérification de la qualité avant la mise en production



Conclusion

- Le projet a permis la définition et le développement de différents algorithmes
- Sur une infrastructure critique en production, le suivi de variables s'est montré prometteur …
- … Mais pas complètement opérationnel
- Nous avons lancé un nouveau projet pour poursuivre la recherche et le développement de ce type d'algorithmes

Merci de votre attention