RAILENIUM TEST & RESEARCH CENTRE	**VACANCE DE POSTE** **Réf. : IMT Railenium**

Titre de la fonction	**POST-DOCTORANT – ANALYSE DE DONNEES POUR DES APPLICATIONS DE CYBERSECURITE** **PROJET X2RAIL-1 / WP8**

Département :	Direction Innovation R&D	**Type de contrat :**	CDD
Superviseur direct : **Encadrant scientifique :**	É. Masson A. Fleury, S. Lecoeuche	**Temps de travail :**	13 mois
Localisation du poste :	Douai (locaux de l'IMT Lille Douai)	**Statut :**	Post-doctorant
Début souhaité :	01-05-2017	**Rémunération :**	~35 k€

Contexte

L'Institut de Recherche Technologique (IRT) Railenium a pour ambition d'être dans le peloton de tête mondial des organismes de recherche et développement, de tests et d'homologation dans le domaine ferroviaire. Railenium se met au service de la filière ferroviaire pour développer l'innovation collaborative et accélérer le développement de nouvelles solutions. Railenium s'appuie sur la mise en commun de compétences et de moyens humains, financiers et matériels par ses 28 membres : gestionnaires de réseaux (SNCF et Eurotunnel), entreprises de la filière (équipementiers, systémiers, ingénieristes, constructeurs), organismes de recherche et universités. Ses activités couvrent le transport urbain, conventionnel et à grande vitesse.

À travers le consortium SmartRaCon, composé du centre de recherche DLR (leader du consortium), du centre de recherche CEIT et de la société britannique NSL, Railenium est un membre associé de l'IP (Innovation Programme) 2 (Advanced Traffic Management and Control Systems) de l'entreprise commune Shift2Rail. SmartRaCon est le seul membre venant du monde académique.

Les activités de l'IP2 ont démarré en septembre 2016 à travers le projet « X2Rail-1 », qui implique 19 partenaires du secteur ferroviaire venant de 9 pays (France, Allemagne, Belgique, Grande Bretagne, Suède, Espagne, Italie et République Tchèque). Le projet couvre différents sujets à travers 6 workpackages (WP) techniques :

- WP3 : Adaptable Communication System
- WP4 : ATO over ETCS
- WP5 : Moving Block
- WP6 : Zero On-Site Testing
- WP7 : Smart Wayside Objects
- WP8 : Cyber Security

Railenium est impliqué sur 3 de ces WPs : WP3, WP6 et WP8.

Contexte du travail :

Ce post-doctorat de 13 mois s'inscrit dans le cadre du projet « X2Rail-1 ». Il sera financé par l'IRT Railenium avec un encadrement scientifique assuré par l'IMT Lille Douai. Dans ce projet, le WP8 traite des aspects de cybersécurité liés aux réseaux ferroviaires. Les contributions de Railenium concerne à la fois les aspects bas-niveau des attaques (niveau signal) mais également les aspects haut-niveau (niveau application) pour la partie sans fil des systèmes de communication ferroviaire. Pour ce poste, le travail sera focalisé sur les données de haut niveau. Une partie du travail sera consacré au développement de stratégies de détection, de prévention et de réponse aux attaques sur le système ferroviaire à travers une structure « Open Pluggable Framework ».

Missions

Description du travail :

Dans le contexte du WP8 du projet « X2Rail-1 », le candidat sélectionné sera en charge :

- D'étudier des algorithmes de classification pour la détection et l'identification des attaques dans un réseau de données ferroviaires ;

- De mettre en place des indicateurs clés pour la détection et le monitoring des attaques et des intrusions ;
- D'implémenter une architecture de décision et d'évaluer ses capacités et performances à travers différents scénarios ;
- De participer à différentes réunions de coordination ;
- De participer éventuellement aux meetings du projet avec les partenaires européens ;
- De contribuer à la rédaction de livrables et de publications scientifiques.

Mission détaillée :

Les travaux à réaliser consistent à investiguer l'utilisation d'algorithmes de classification adaptatifs pour la détection et l'identification des attaques sur un réseau de données ferroviaires.
Ce travail permettra de : (1) détecter des (nouvelles) attaques et intrusions internes ou externes, (2) construire des modèles avec une connaissance incomplète des modes normaux et sécurisés, (3) adapter les modèles mis en place pour changer les comportements des attaqueurs voulant briser les règles de sécurité.
Dans un tel système, des règles basiques sont codées dans une première initialisation du système. Le système de détection des attaques va ensuite surveiller et analyser tout type de dérive possible dans le comportement de l'opérateur pour détecter et localiser les attaques plus précisément.
Dans ce travail, la partie décision s'appuiera sur des caractéristiques extraites du signal et/ou des données. La première étape consiste à déterminer, à l'aide de spécialistes de sécurité opérationnelle, les paramètres importants à prendre en compte (statistiques, paramètres linéaires/non linéaires, paramètres fréquentiels ou temps/fréquence, évolution d'une période de temps à une autre, *etc.*) Une fois définis, les modèles seront construits en utilisant ces attributs (ou une partie de ces attributs s'ils sont trop corrélés ou identifiés comme non pertinents par l'analyse de données) et pris en compte dans les évolutions temporelles et les changements dynamiques. À partir de ces modèles et des flux de données, nos algorithmes adaptatifs peuvent rapidement classifier les périodes de temps comme normales ou ayant été atteintes par une attaque.
Pour cette partie d'analyse de données, des données de simulation acquises sur différentes plateformes des partenaires Railenium pourront être utilisées pour travailler sur des cas d'usages spécifiques (attaques particulières).

Compétences

Savoir	Savoir être
Doctorat en analyse des données et modélisation expérimentale Compétences en logiciels d'analyse de donnée (R, SPSS, Weka, Matlab, Scikit Learn, …) Anglais courant	Sens de l'initiative Autonomie/travail d'équipe Excellent relationnel Créativité, rigueur, organisation Capacité d'autoformation Esprit de synthèse, réactivité Disponibilité (des déplacements à prévoir) Excellentes capacités rédactionnelles

Les candidatures (lettre + CV) sont à adresser dans les plus brefs délais par courrier électronique, sous la référence IMT Railenium, à emilie.masson@railenium.eu, anthony.fleury@mines-douai.fr, stephane.lecoeuche@mines-douai.fr