Projet de sécurité réseau

Date de lancement	• 13 décembre 2018
Date limite pour présenter une demande	• 24 janvier 2019
Énoncé de problème	La 5G est une technologie prometteuse qui prendra en charge de nouveaux types de communications sans fil notamment depuis les appareils de l'Internet des objets (IdO) et de machine à machine. Cela étant dit, il est évident que les mécanismes de sécurité d'aujourd'hui, qui dépendent beaucoup des interventions humaines, ne pourront s'adapter aux nouvelles technologies sans fil. Il faut donc mettre au point des solutions automatisées pour (1) détecter et identifier les menaces et les fuites de données et (2) les atténuer à l'échelle du réseau. Le projet de sécurité réseau vise la conception de méthodes qui automatisent la sécurité réseau. Nous croyons qu'à ce titre les technologies d'apprentissage automatique peuvent constituer une bonne solution et souhaitons étudier les moyens de les utiliser pour automatiser la sécurité réseau.
Partenaire de projet	• Ciena
Échéancier	• Deux (2) ans
Financement disponible	• Jusqu'à 130 000 $ CA
Type de demandeur	• Université ou collège de l'Ontario
Endroit	• En Ontario
Renseignements sur le projet	Les mécanismes traditionnels de sécurité de l'information fonctionnent en refusant l'accès à des actifs essentiels au moyen de fonctionnalités complémentaires, comme les pare-feu réseau, les systèmes de prévention des intrusions, les anti-maliciels en mode hôte et les services de mandataire. Ces méthodes détectent les activités malveillantes associées au mauvais trafic connu et les bloquent en les mettant sur une liste noire ou appliquent plusieurs règles, qui restreignent le flux de données en fonction des hôtes sources et de destination et des ports et protocoles prévus. L'évolution des architectures modernes afin d'intégrer l'infonuagique et l'arrivée des appareils dotés d'une connexion Internet (IdO) font en sorte que ces approches sont de moins en moins efficaces et extensibles. Pour résoudre ce problème, nous nous penchons sur une méthode reposant sur l'établissement d'une liste blanche qui élimine le besoin d'avoir des dispositifs de sécurité distincts et intègre la sécurité à même l'architecture réseau. Cette méthode pourrait notamment fonctionner sans pare-feu. Contrairement aux solutions actuelles qui utilisent des pare-feu, nous proposons que la confiance accordée à un appareil soit établie par un appareil périphérique connecté. Selon cette méthode, un classificateur reposant sur l'apprentissage automatique indique au réseau ce à quoi il peut faire confiance. Le réseau exerce une surveillance continue du comportement des périphériques et les classe dans la

	catégorie « de confiance » ou la catégorie « suspect ». Le classement du trafic se fait au moyen d'un « classificateur de trafic réseau » fondé ou non sur l'apprentissage automatique. De plus, on devrait pouvoir catégoriser les microservices en nuage de confiance à l'aide de méthodes similaires. À cette fin, nous avons besoin d'un partenaire du milieu de l'enseignement pour effectuer la recherche relative aux algorithmes d'apprentissage automatique. Nous avons également besoin d'un partenaire du milieu de l'enseignement qui s'y connaît en cybersécurité, pour nous assurer de rechercher les activités « suspectes » pertinentes, p. ex., les fuites de données, les voies clandestines et les tentatives d'intrusion. Leurs efforts doivent permettre la mise au point d'algorithmes d'apprentissage automatique et de techniques de formation servant à classer le comportement au point terminal comme étant digne de confiance ou suspect. Le partenaire du milieu de l'enseignement devra proposer et évaluer d'autres méthodes de classification avec et sans supervision. Les données d'entrée du classificateur peuvent être des en-têtes de paquet obtenus par inspection approfondie des paquets (IAP); quant au classificateur, il peut s'appuyer sur la détection des écarts par rapport à certains protocoles réseau. Le partenaire du milieu de l'enseignement doit être en mesure de fournir un environnement de simulation ou d'émulation, qui sera utilisé par la suite pour générer une interaction d'appareils « normaux » et « malveillants » sur le réseau. Cette interaction servira à la formation relative aux modèles d'apprentissage automatique et à leur évaluation.
Objectifs du projet et résultats escomptés	La réalisation de ce projet occupera deux doctorants pendant deux (2) ans. Par conséquent, nous nous attendons à ce que ces travaux de recherche donnent lieu à la publication d'au moins trois (3) articles de revues et d'au moins quatre (4) articles à l'occasion de congrès. Le projet a aussi comme objectif la livraison d'un prototype fonctionnel qui sera exécuté sur le banc d'essai du projet ENCQOR. Cet objectif est conditionnel à la résolution des problèmes de recherche sous-jacents et à la disponibilité des outils d'automatisation nécessaires sur le banc d'essai d'ENCQOR.
Capacités des demandeurs	Les demandeurs doivent être en mesure de céder à Ciena les éléments de propriété intellectuelle découverts dans le cadre du projet. Doctorants • Au moins deux (2) doctorants disponibles pour mener les travaux de recherche. • Les étudiants doivent connaître les concepts de réseautique. • Les étudiants doivent être à l'aise avec la simulation des protocoles réseau. • Les étudiants doivent avoir une connaissance approfondie de la statistique et de solides compétences en mathématiques. • Les candidats doivent pouvoir utiliser de façon indépendante des progiciels ouverts (TensorFlow, MXNet, scikit-learn) afin de développer des simulations d'apprentissage automatique. **Chercheurs principaux** Compétences en apprentissage automatique appliqué

	• Compréhension globale de l'IA et de l'apprentissage automatique. • Expérience dans l'application d'algorithmes d'apprentissage automatique. • Connaissance de l'exploration et de l'analytique de données • Connaissance de l'ingénierie de concept. Compétences en sécurité • Expérience de recherche relative aux cybermenaces. • Expérience de recherche en détection de voies clandestines au sein d'environnements répartis.