ENCQOR 5G **Technology Development Program [SME Stream]**

Anchor Firm	ciena
Challenge Statement	**Classification of traffic anomalies with Machine Learning**

Challenge Launch Date	June 18, 2020
Challenge Deadline	July 16, 2020
Challenge Statement	Understanding traffic patterns is mission-critical for Network Service Providers. A part of it is traditionally addressed with statistical methods that simply report abnormal deviations from an expected baseline. But when a traffic shift is observed, is it problematic or is it seamless for the network operator? Is it legitimate or accidental or malicious? We are looking to develop a next-generation traffic-pattern classifier based on ML algorithm(s) that will provide richer insights about the root-cause and service-impact of traffic anomalies. The classifier will leverage state-of-the-art machine learning algorithm(s) trained with large data sets of traffic flow records linked with other data sources relevant for telecommunications network operations.
Project Partner	Ciena Canada
Timeline	• up to 12 months [NOTE: Projects must be completed by March 31, 2022, no extensions will be available beyond this timeline]. • Project expected to start in Fall 2020
Available funding	Up to $470,000.00 CDN
Applicant Type	Ontario based SME Scale company
Location	Ontario

Project Details	• Ciena will provide anonymized datasets collected with its Blue Planet Route Optimization and Analysis (ROA) product
	• The SME will work with Ciena's data science and ROA experts to develop a comprehensive analysis of the above data
	• The data analysis should be able to:
	  ○ process raw inputs from different sources and output data files consumable by ML
	  ○ discover the main types of traffic patterns (possibly with unsupervised or self-supervised learning or clustering)
	  ○ correlate traffic shifts with routing events
	  ○ develop a data-labeling strategy for each type of pattern
	  ○ develop state-of-the-art classifier algorithm that learns to recognize the main types of traffic patterns with good sensitivity and good precision
	  ○ optimize the classifier to detect DDoS attack patterns with maximal sensitivity and precision

Project Goals/ Outcomes	• SME will deliver: ○ written report sumarizing the results of the above analysis

	○ open source code to reproduce all the above results ○ actual ML model persisted as ONNX file ○ knowledge transfer to ensure Ciena staff is able to reproduce the results from the delivered code • Intellectual Porperty ○ Ciena owns its background IP ○ SME owns its background IP ○ Ciena owns foreground IP directly related to this project ○ SME may own other IP developed as a side-effect of this project, but not directly overlapping with it
Applicant Capabilities	• Cutting-edge expertise with supervised and unsupervised Machine Learning, and with deep learning • Proficient with Python machine learning ecosystem (SciKitLearn, xgBoost, Keras, TensorFlow, pyTorch) • Experience with IP network data is an asset