5G (ENCQOR) Technology Development Challenge Statement

Network security project

Challenge Launch Date	• December 13, 2018
Deadline for Open Call Applications	• January 24, 2019
Challenge Statement	5G is promising to enable new forms of wireless communications, namely internet-of-things (IoT) devices and new machine-to-machine (M2M) communications. With this in mind, it is clear the today's security mechanisms which are heavily dependent on human input are not going to scale with new wireless technologies. Automated solutions are needed to (1) detect and identify threats and data leaks and (2) mitigate them in the network. The network security project aims to devise approaches that automate network security. We believe that machine learning technologies may provide a good solution in this respect and would like to investigate how to use them to automate network security.
Project Partner	• Ciena
Timeline	• 2 years
Available funding	• Up to $130 000 CDN
Applicant Type	• Ontario based university
Location	• Ontario
Project Details	Traditional information security works by denying access to critical assets through add-on functionality to include network-based firewalls, intrusion prevention systems, host-based malware protection, and proxy services. These approaches look for malicious activity matching known bad traffic and block it, known as blacklisting, or they require multiple rules to be implemented which specifically allow a data flow based on source/destination hosts and expected port and protocol. The change in modern architectures to include cloud and the influx of Internet enabled devices (IoT) make this traditional approach increasingly ineffective and unscalable. We are investigating a white-listing approach to the problem, which eliminates the need for separate security devices and integrates the security into the network infrastructure directly. A possible outcome of this approach is to eliminate the need for firewalls entirely. Comparing to the current solutions using firewalls, we propose that trust for a device be established by the edge network device. Trust is learned by the network with a machine learning classifier. The network is constantly monitoring the behavior of the network devices for the purposes of classifying them as "trusted" or "suspicious". The classification of the traffic is performed with a "network traffic classifier", which may be based on machine learning technology. We expect that similar methods can be used to establish trust for cloud-based micro-services as well.

	We are looking for an academic partner to perform research in machine learning algorithms for this purpose. We also need an academic partner with knowledge of cybersecurity to ensure that we are researching relevant "suspicious" activities, e.g. data leaks, covert channels, intrusion attempts. We expect the academic effort to devise machine learning algorithms and training techniques to classify the end-point as trusted or suspicious. We expect the academic partner to propose and evaluate alternative supervised or unsupervised methods for the classification. The input to the classifier may be packet headers obtained by deep packet inspection (DPI) and the classifier itself may rely on detecting deviations from certain network protocols. We expect the academic partner to provide a simulation or an emulation environment, which we would be used to generate network interaction of "normal" and "malicious" devices and use this for training and evaluation of machine learning models.
Project Goals/ Outcomes	We expect this project to consume the time of at least two PhD candidates over a period of 2 years. As such, we expect this research to result in at least four conference and three journal publications. Another goal of the project is to deliver a working prototype of the research to run on the ENCQOR testbed. This goal will be subject to successfully solving the underlying research problems and the availability of appropriate automation tools on the ENCQOR testbed.
Applicant Capabilities	Applicants should be able to assign any intellectual property discovered during this project to Ciena. PhD Candidates • Minimum 2 candidates available to perform the research • Students should have knowledge of networking concepts • Students should be comfortable with network protocol simulations • Students should have strong statistical knowledge and mathematical abilities • Candidates should be able to independently use complex open-source packages (TensorFlow, MXNet, scikit-learn) to develop machine learning simulations **Principal investigator(s)** Applied machine learning expertise • Comprehensive understanding of AI & Machine Learning • Experience applying machine learning algorithms • Data mining and data analytics • Feature engineering Security expertise • Research experience with cybersecurity threats • Research experience in detection of covert channels in distributed environments

Statement about next steps with links to program guidelines and application portal- TBC