Machine Learning for Detecting Internet Traffic Anomalies

Prof. Ljiljana Trajković

Abstract:
Border Gateway Protocol (BGP) enables the Internet data routing. BGP anomalies may affect the Internet connectivity and cause routing disconnections, route flaps, and oscillations. Hence, detection of anomalous BGP routing dynamics is a topic of great interest in cybersecurity. Various anomaly and intrusion detection approaches based on machine learning have been employed to analyze BGP update messages collected from RIPE and Route Views collection sites. Survey of supervised and semi-supervised machine learning algorithms for detecting BGP anomalies and intrusions is presented. Deep learning, broad learning, and gradient boosting decision tree algorithms are evaluated by creating models using collected datasets that contain Internet worms, power outages, and ransomware events.

Short bio:
Ljiljana Trajkovic received the Dipl. Ing. degree from University of Pristina, Yugoslavia, the M.Sc. degrees in electrical engineering and computer engineering from Syracuse University, Syracuse, NY, and the Ph.D. degree in electrical engineering from University of California at Los Angeles. She is currently a professor in the School of Engineering Science, Simon Fraser University, Burnaby, British Columbia, Canada. Her research interests include communication networks and dynamical systems. She served as IEEE Division X Delegate/Director and President of the IEEE Systems, Man, and Cybernetics Society and the IEEE Circuits and Systems Society. Dr. Trajkovic serves as Editor-in-Chief of the IEEE Transactions on Human-Machine Systems and Associate Editor-in-Chief of the IEEE Open Journal of Systems Engineering. She is a Distinguished Lecturer of the IEEE Circuits and System Society, a Distinguished Lecturer of the IEEE Systems, Man, and Cybernetics Society, and a Fellow of the IEEE.