COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Chad L. Calvert

for the degree of Doctor of Philosophy (Ph.D.)

"Data Collection Framework and Machine Learning Algorithms for the Analysis of Cyber Security Attacks"

July 1, 2019, 11:30 a.m.
Engineering East, Room 405
777 Glades Road
Boca Raton, FL

DEPARTMENT:
Computer and Electrical Engineering and Computer Science

ADVISOR:
Taghi M. Khoshgoftaar, Ph.D.

PH.D. SUPERVISORY COMMITTEE:

Taghi M. Khoshgoftaar, Ph.D., Chair
Bassem Alhalabi, Ph.D.
Xingquan Zhu, Ph.D.
Dingding Wang, Ph.D.
Mehrdad Nojoumian, Ph.D.

ABSTRACT OF DISSERTATION

The integrity of network communications is constantly being challenged by more sophisticated intrusion techniques. Attackers are shifting to stealthier and more complex forms of attacks in an attempt to bypass known mitigation strategies. Also, many detection methods for popular network attacks have been developed using outdated or non-representative attack data. To effectively develop modern detection methodologies, there exists a need to acquire data that can fully encompass the behaviors of persistent and emerging threats. When collecting modern day network traffic for intrusion detection, substantial amounts of traffic can be collected, much of which consists of relatively few attack instances as compared to normal traffic. This skewed distribution between normal and attack data can lead to high levels of class imbalance. Machine learning techniques can be used to aid in attack detection, but large levels of imbalance between normal (majority) and attack (minority) instances can lead to inaccurate detection results.

In this dissertation, we propose a framework for the collection of five network attack datasets. Our capture procedure allows for the collection of real-world representative data using a live, full-scale network environment. For each of our datasets, we evaluate unique traffic behaviors and key discriminating features that can aid in attack detection. We apply a variety of machine learning algorithms to our application layer attack datasets to evaluate detection performance. As several of these datasets are categorized as big data with high levels of class imbalance, we also investigate the use of random undersampling towards the mitigation of class imbalance. Our results show that overall, the use of random undersampling significantly improves classification performance for highly imbalanced data sets. A comparative analysis of performance metrics is also performed to identify the effectiveness of using certain metrics for the evaluation of highly imbalanced big data. We further sought to improve our performance metrics through the application of a novel threshold-based optimization approach. Based on our results, we propose that the use of a singular metric for evaluating highly imbalanced big data may be ineffective, and the evaluation of multiple metrics can offer substantial insight into the true performance of a given model.

BIOGRAPHICAL SKETCH
Born in Garland, Texas
B.S. 2008, Florida Atlantic University, Boca Raton, Florida
M.S. 2009, Florida Atlantic University, Boca Raton, Florida
Ph.D. 2019, Florida Atlantic University, Boca Raton, Florida

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: 2015 - 2019

Qualifying Examination Passed: Fall 2014
Selected Published Papers:

C. Calvert, T. M. Khoshgoftaar, C. Kemp, and M. M. Najafabadi. A framework for capturing http get ddos attacks on a live network environment. In 23rd ISSAT International Conference on Reliability and Quality in Design, 7 pages, 2017.

C. Calvert, T. M. Khoshgoftaar, M. M. Najafabadi, and C. Kemp. A procedure for collecting and labeling man-in-the-middle attack traffic. International Journal of Reliability, Quality and Safety Engineering, 24(1):19 pages, 2017.

C. Calvert, T. M. Khoshgoftaar, C. Kemp, and M. M. Najafabadi. Detection of Slowloris Attacks Using Netflow Traffic. In 24th ISSAT International Conference on Reliability and Quality in Design, 6 pages, 2018.

C. Calvert, T. M. Khoshgoftaar, C. Kemp, and M. M. Najafabadi. Detecting Slow HTTP POST DoS Attacks Using Netflow Features. Proceedings of the Thirty-second International Florida Artificial Intelligence Research Society Conference, 4 pages, 2019.

C. Calvert, T. M. Khoshgoftaar. Impact of Class Distribution on the Detection of Slow HTTP DoS Attacks using Big Data. Journal of Big Data, 18 pages, 2019 (Under Review).